

Process Control Systems Forum
2005 Spring Meeting

MEETING MINUTES

Meeting:	Process Control System Forum Spring Meeting (Dallas, TX)
Date:	May 18, 2005
Session:	A Consolidated Security Mechanism for the Entire Utility Enterprise
Presenter:	Chair – Jay Wack
Type:	Presentation

Agenda

Attachments

https://www.pcsforum.org/events/2005/spring/breakout_session/Tec%20Sec_Wack.pdf



Group discussion

The presenter, Jay Wack, delayed the session start until 13:07 because so few people were present after lunch at 13:00. By the end of the session, the total attendance was about twice that at the start.

A 10 MB augmented and reordered set of slides were presented that were put on the conference desk laptop.

The presenter described the underlying problem of constrained information sharing that is encountered by modern IT-enabled corporations. This problem is that a single set of information needs to be shared with different groups, each with their own rights to view of a subset of the information. Both data at rest and data in transit need to be protected. Traditional uses of cryptography address only the data in transit issue.

Additional slide 1:

COMSEC is traditional point to point.

INFOSEC needs to be protecting the information itself, not the channel. Information is stored by content, with signatures to provide validation of content:

1. Self protecting data objects
2. Data label awareness
3. Data label aware services
4. Identity management augmented by
5. Key Management that is
 - a. role based
 - b. fine grained (objects)
 - c. dynamic, not static, keys



Process Control Systems Forum 2005 Spring Meeting

Additional slide 2:

Started with ANSI X9.69, which is a process called CKM (constructive key management) that provides role-based access control (RBAC) enforced by cryptography
Published as ANSI Standards

- o X 9.69 Framework for key management extensions
- o X9.73 Cryptographic message syntax
- o X9.96 Secure XML
- o Properties of CKM approach:
- o Key material not specific to individuals
- o Addresses the one-to-many distribution problem of key management
- o Access privileges bound to data via cryptography
- o Built-in key recovery performed by system owner
- o Modeling Role-Based Access Control (RBAC)
- o Context-based security
- o Complementing PKI

Additional slide 3: Permissions matrix

(DoD example showing three segments, one for intel aspects, one for personnel aspects, one for war fighter aspects. Each segment showed a large matrix of different access classes, where each individual set of alternatives -- e.g., UNCLASSIFIED, CONFIDENTIAL, SECRET, TOP SECRET - - specifies just a single class.)

Additional slide 4: CKM object and header: digital rights management

There was a spirited discussion throughout the presentation, with a number of questions about details such as the difficulty of applying this style of rights management to existing databases. "Anything that is digital and that can be named can be controlled by this solution." It does not require changes in the existing corporate system, but just application of rights to selected elements of the enterprise's information base.

The presenter then took questions. The following summary coalesces answers that occurred at different times during the Q&A period.

1. Q: SCADA systems have very short messages. How does this technology apply to that case?
A: That can be a problem for some devices, but there are existing systems where this is in use. There are some cases where a low data rate and high polling rate does not permit this solution.
2. Q: How will you supply a device-to-device key?
A: Today's solution uses a smart chip that authenticates access to the device through its maintenance port. The presenter gave examples of rights management.
3. Kevin Stagg's statement: "You need to move your systems to the level where every object carries permissions and every use of an object is validated by those permissions."
4. Tom Phinney statement: "With adequate caching in the endpoint devices, there should be no message extension except for cryptographic synchronization and extended protection for the current short CRCs."

Decisions and Action Items

