From Physical to Fine-Grained Security

William Cox
Cox Software Architects LLC
OASIS Technical Advisory Board Co-Chair
wtcox@CoxSoftwareArchitects.com
http://www.CoxSoftwareArchitects.com

Motivation

- CIA Reports Cyber attacks on Grid/Utilities
  - http://www.pcworld.com/article/141564/cia_says_hackers_have_cut_power_grid.html
  - Multiple instances
  - Primary motivation: extortion
- Opening access requires controlling access
- Great value in applying eCommerce mechanisms to energy and building management
- We can't just bar the door any more…
  - Access to internet information
  - Distributed control
  - More complex control characteristics

OASIS

Background

- Concerned with distributed applications
- Enterprise character
- Accessible to the right people and software
- Information integrity
- eCommerce and enterprise requirements

OASIS

Security Services

- Authentication – confirm asserted identity
- Authorization – permit or deny a request
- Integrity – prevent undetected modification of data
- Confidentiality – prevent unauthorized reading of data
- Audit – preserve evidence for accountability
- Administration – control configuration
- Others …

OASIS

Why Fine-Grained Access?

- De-perimeterization
  - No longer just “them and us”
  - Firewall is no longer sufficient
  - Eggshell-like brittleness, soft unprotected contents
- Service Oriented Architectures
  - Multiple access contexts for each service
- Software as a Service
  - Complex interactions of internal and external components
- Grid security needs are evolving as eCommerce needs have evolved
  - Leverage technology experience and architecture
  - Similar issues

OASIS

Why OASIS?

- Leader in Web Services and XML
  - eCommerce, Universal Business Language, Open Document Format, UDDI, oBIX, and more
- Open and transparent process
  - Free access to standards and work in progress
  - http://www.oasis-open.org is the entry point
  - Improve your ROI with high quality standards
    - see “Value” at http://www.oasis-open.org/webinars/
- Broad technology industry support
- Energy and Buildings focus area developing
- Interoperate with confidence
  - Security, data integrity, transaction processing, reliable messaging. ebXML, …

OASIS

OASIS and Security

- Standards and Technical Committees include
  - WS-Security (Web Services Security)
  - SAML (Security Assertion Markup Language)
  - XACML (eXtensible Access Control Markup Language)
  - WS-Trust
  - WS-SecureConversation
  - WS-SecurityPolicy
  - WS-Federation
  - Biometric Identity Assurance
  - Identity Metasystem Interoperability – Information cards, ID systems
  - Emergency Management (Alerting, Distribution Element, Hospital Availability – Adopted by Open Geospatial Consortium)
- Key notion: Separation of policy and mechanism

OASIS

Web Services Security

- WS-Security – Standards for Interoperability
  - Between entities, not internal behavior
  - Authentication, Integrity, Confidentiality, Key Exchange
- Consistent with XML, SOAP, WSDL, WS-Policy
  - Separates policy from mechanism
- Supports multiple infrastructure types
  - Passwords, X.509, Kerberos, SAML, etc.
- Enables enterprise security
  - Most of WSS is not about *stronger* security
  - Better scaling, easier deployment

OASIS

WS-Secure Conversation

- Similar to SSL – endpoints have secure session for information exchange
- Two party and three party
- More efficient and secure than using long term secrets directly
- Builds on WS-Security and WS-Trust
- Use with WS-ReliableMessaging for secure and reliable end-to-end interactions

OASIS

Summary

- eCommerce knowledge, architecture, and technologies transfer well to Grid and Building management
- OASIS is a great place to apply fine-grained security and eCommerce and Emergency Management and…
- Improve your Return on Investment and quality of security by
  - applying high quality standards
  - building new ones

OASIS

References

- Email
  - wtcox@CoxSoftwareArchitects.com
- Talks on energy management, eCommerce, standardization, project planning. Newsletter (site update in progress)
  - http://CoxSoftwareArchitects.com
  - http://CoxSoftwareArchitects.com/energy (28 Sept 2008)
- OASIS home page - standards, TC list links in left navigation bar
  - http://www.oasis-open.org/
- OASIS and XMLTechnologies Analysis & Information
  - http://www.xml.org
  - http://xml.coverpages.org/