

HDV407: Enforcing Content security in a collaborative environment

Robert Ginsburg

Version3, Inc.

<mailto:robert.ginsburg@ver3.com>

Agenda

- Collaborative security
- Authentication vs. authorization
- Audit trails
- Immutable content
- Runtime policy enforcement
- Simplifying security constructs
- Security watchdog

Challenges of collaborative security

- Most systems (including SharePoint) require discrete security structures
- Collaboration tends to require ad-hoc relationships
- Technology must blend the perspectives in a way that users understand

Authentication

- **Authentication is not authorization**
 - Nothing should be implicitly granted to “authenticated users”
- **Authentication must be layered to distinguish and protect types of resources**
 - Extranet logon must not have access to LAN logon
- **Security principals must be persistent**
 - Audit trails are useless without a persistent reference

Content level authorization

- Document based rights management
- Follows the document , not the user
- For Office documents
 - RMS (sp2) provides rights management protection for documents injected at download
 - Rules operate for Office clients,
 - Content is NOT Immutable

Immutable content

- Even with good audit trails, content can leave the system
 - RO content should be stored in an immutable format :
 - PDF for electronic records
 - Partial support in Microsoft IRM services
 - Other vendors exist ..
 - RW content should be versioned ..with previous versions made immutable

Simplifying security constructs

- Most users find ACL's difficult to understand
- Our users find SharePoint roles difficult to understand
- Need a simple construct
 - I share with you, us
 - I give to you, you give to me
 - Etc.

Our Scenario

- Students must have RW access to their work-in-progress homework
- Parents and advisors must have RO access to relevant work-in-progress homework
- Students, educators and parents must have RO access to relevant student submitted homework

Our Scenario

- Students must not have access to other student submitted homework
- Parent relationship may change at any time
- Class groups may change at any time
- Parents must not have LAN access to network devices

Our Scenario

- Students should be able to share some content with other students
- Students must have at least RO access to all content they author
- Principal must have “observer” access to entire system regardless of author or authoring tools

Solutions – runtime enforcement

- Runtime engine watches for security changes in student store
 - Site permissions
 - Site groups
- Adjusts permissions on site and lists so that appropriate individuals can always access content.
 - Evaluate parent/student relationship
 - Evaluate advisor/student relationship

Runtime enforcement

DEMO

with code reviews

Solutions – simplified security

- Provide simplified UI that allows grouping and protecting content rendering
 - Wraps web part rendering
 - Collaborative UI security (not content ACL)
 - Easy for student and teacher to understand
 - One-to-one relationship

Simplified security

DEMO

with code reviews

Solutions – changing security constructs

- Watchdog engine watches for relationship changes and content changes
 - Student/Parent , Student/Class & Educator/Class
- Reevaluates individual permission on all impacted items
 - Impersonates student for content query
 - Projects rules for each item and modifies ACL

Security watchdog

DEMO

with code reviews

Solution – Principal as global observer

- **Role based Impersonation (“ViewAs”)**
 - AD group membership grants base permission
 - AD group membership grants specific permission
- **User Is authenticated , authorized and transformed into target user**

Observer mode

DEMO

Solution – Parents must not access LAN devices

- Authentication is managed externally by parent
- Parent session object is linked to AD principal at logon
- Parent/Learner relationship managed on AD principal object

Identity firewall / Parent relationship

DEMO

SharePoint SPUser connendum

- SPUser is a numeric ID relative to Site
- SPFieldUserValue is based on SPUser
 - Does not retain “deleted or disabled accounts”
 - Authentication scope is SharePoint site collection
- **MUST BE RERECONCILED FOR EVERY EVALUATION**

SharePoint SPUser connendrum

DEMO

with code reviews

Things we did not review

- **Immutable content**
 - Transform to alternate format on submission
 - DRM / SharePoint integration
- **Access audit trails**
 - Audit trails provide proof of system access only if the security principal definition is persistent (don't delete accounts !)
- **SharePoint internal security constructs**
 - Groups, roles, etc.

Review & Resources

- Security is not just ACL
- Collaborative context is shared and not always easily understood
- Authentication is not implicit permission!
- Code samples available at:
<http://files.ver3.com>

Your Feedback is Important

Please fill out a session evaluation form and either put them in the basket near the exit or drop them off at the conference registration desk.

Thank you!