Heterogeneous Identity and Access Management for Microsoft Office SharePoint Server

Neil Readshaw, Tivoli Advanced Technology Group
Nataraj Nagaratnam, Distinguished Engineer, Tivoli Security
From this presentation you will...

• Understand the business context for the challenges in securing Microsoft SharePoint

• Gain an appreciation of Microsoft SharePoint and its security model

• Understand the value in integrating Microsoft SharePoint with Tivoli Security solutions

• Appreciate the available integration alternatives and how to decide between them

• See a demonstration of some of the newest integration capabilities
Agenda

• Security challenges in collaboration environments

• SharePoint overview and use cases

• Demo

• Summary
Security challenges in collaboration environments
Business environments are collaborative and dynamic

• In increasingly rich and dynamic ways, businesses need to:
  – Connect people, applications and information
  – Provide access to information – to the right people, at the right time

• Business requires
  – Visibility
    • How do you know who accessed what?
  – Control
    • How to identify people and determine the trustworthiness of their identification?
    • How to restrict access to confidential information to authorized users?
  – Automation
    • How to automatically provision identities and credentials based on roles?
Collaborative Intranet – share information, blog,..

- How to manage the identity lifecycle?
- How to control access based on context?
- How to propagate identity to heterogeneous web applications and services?
Extranet Portal – access to confidential information, collaborate with partners...

- How to achieve SSO within and across organizations?
- How to provide entitlements and access based on application context?
- How to audit user activity?
IBM’s identity and access management strategy delivers identity governance using policy management.

Identity Governance using Policy Management

People
- Business Roles
- Users

Applications
- Entitlement
- Application Roles

Data
- Unstructured Data
- Structured Data

Monitoring
User activity monitoring and conformance to policy and regulations
SharePoint is...

Microsoft Office SharePoint Server (MOSS)

Windows SharePoint Services (WSS)

ASP.NET

SSO

Audit

IIS

Authn

Role

Windows Workflow Foundation

Entitlements and Access

.JSON Framework

Identity

Profile

SQL Server

Windows Server

Active Directory
SharePoint Security Challenges

• Many SharePoint deployments started as tactical solutions within workgroups / lines of business
  – These deployments are becoming more strategic
  – New strategic deployments are also increasing
• SharePoint provides auditing, but not compliance and reporting management in the broader context
• Granular or complex access control is difficult to achieve
  – Authorization and entitlement management based on contextual information (about users, resource, environment) is limited
• Unified management of identities, claims and access policies across heterogeneous enterprise infrastructure is necessary
  – SharePoint is one system in the environment
Web SSO Integration using Tivoli Federated Identity Manager

- Maximize use of Active Directory for authentication
  - Well suited to intranet scenarios
- TFIM Runtime deployed on a Windows system in the AD environment

1. Request service ticket for WebSEAL
2. SPNEGO (Kerberos over GSS)
3. WS-Trust
4. Request service ticket for IIS/MOSS
5. SPNEGO (Kerberos over GSS)
Web SSO Integration with TAM

- Leverage TAM’s flexible authentication capabilities
- Exploits ASP.NET interface for using TAM as a user registry and decision point for role based access control
- Preferable when SharePoint should use enterprise LDAP directory
Federated Single Sign-on with TFIM

- Simplifies user experience in B2B scenarios
- Provide users with control and consent in B2C scenarios
Entitlement Management using Tivoli Security Policy Policy Manager (TSPM)

• Standards based entitlement management with rich constructs

• Granularity to the document/item level
Identity Lifecycle Management

- Use Tivoli Identity Manager (TIM) for policy driven management of all identities in a SharePoint environment
- Use TIM workflow to align with business processes
- TIM Adapter:
  - Integrates with SharePoint profile database via SharePoint web services
  - Complements existing adapters for Active Directory, TAM, LDAP
Compliance Reporting and Management

- Incorporate SharePoint events into a compliance solution using Tivoli Compliance Insight Manager (TCIM)
- Provides visibility of user activity
  - May be a good way to begin with tactical SharePoint deployments

```xml
<event>
  <when>2009-01-08T15:49:33.0+10:00</when>
  <who realname="SharePoint Administrator"
      logonname="spsadmin"/>
  <what verb="View" noun="List"
         success="success"/>
  <where type="Microsoft Windows"
          name="sps2007.jkenterprises.com"/>
  <whereto type="-" name="-"/>
  <onwhat type="List" path="Reports/Lists"
          name="Sample KPIs"/>
  <info>-</info>
</event>
```
Pulse 2009
Managing the World’s Infrastructure
Demonstration
Extranet Scenario

- Nick, University researcher
- Employees
- Internet
- David, Government agency
- Tom, Industry analyst
- Authn & SSO
- TAM WebSEAL
- SharePoint
- Research Data
- Entitlements
- Tivoli Directory Server
- Tivoli Security Policy Manager
- Tivoli Compliance Insight Manager
- Audit

Pulse 2009
Managing the World’s Infrastructure
Intranet Scenario
Securing the Intranet Scenario

Simplifying the task of getting people access to applications and data

Use of common security services for authentication and entitlement management

MOSS (Wikis, Blogs, Document Libraries)

Active Directory

MOSS DB

Web services

Web applications

TAM TFIM

TSPM

TIM

Identity propagation

Authz

Provisioning
Securing the Extranet Scenario

- Partner Organizations
- FSSO or UCSSO
- TAM WebSEAL
- MOSS (Extranet Portal)
- MOSS DB
- Other Web applications
- MOSS DB
- Partner Organizations
- TAM WebSEAL
- MOSS (Extranet Portal)
- MOSS DB
- Other Web applications
- MOSS DB
- SSO
- Authentication
- TFIM
- Use of common service for entitlement management
- Authz
- TCIM
- Audit

Authentication choices to meet regulations, provide a differentiating user experience

Bring enterprise data in SharePoint within the enterprise compliance regime

Use of common service for entitlement management
Summary

• Securing SharePoint environments is important, and must fit within the broader enterprise security strategy and solutions

• Tivoli offers broad, integrated capabilities that address key concerns in intranet and extranet use cases for SharePoint
  – Addresses Visibility, Control, Automation

• We welcome any opportunity to partner with you to extend these integrations to better meet your requirements
References

• Redpaper: IBM Tivoli Security Solutions for Microsoft Software Environments

• IBM developerWorks: Enabling Microsoft Office SharePoint Server Client Integration through Tivoli Access Manager e-business WebSEAL using Forms Authentication

• IBM developerWorks: Single sign-on from Microsoft Office SharePoint Server to applications

• Tivoli Access Manager integration with Microsoft .NET

• Tivoli Access Manager integration with Microsoft SharePoint Services
Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided “AS IS” without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

© IBM Corporation 1994-2009. All rights reserved.
References in this document to IBM products or services do not imply that IBM intends to make them available in every country.