Identity and Access Management Technologies

Developed By: Janice Moyer

Presented By: Adam James

NebraskaCERT - 8/14/2007

Access Control Process

- Identification
  - Ensuring the subject is who he claims to be
- Authentication
  - Subject provides additional information in addition to the identity to gain access
- Authorization
  - Subject has the necessary privileges or rights to access the requested asset

All Rights Reserved, Continuum Worldwide, 2007

Identification Technologies

- Metadirectories
- Virtual Directories
- Federated Identity Management
- User Provisioning

All Rights Reserved, Continuum Worldwide, 2007

Metadirectories

- Software products that synchronize and optionally aggregate identity data stored in multiple repositories.
- Used to reduce the cost of user administration
- Utilize in some cases rather than user provisioning products
- Use with directory integration products to provide synchronization to other identity stores
- Vendors
  - IBM, Microsoft, Novell, Sun

All Rights Reserved, Continuum Worldwide, 2007

Virtual Directories

- Creates a logical (virtual) view of a directory but does not contain any data itself
- The purpose is to combine data from multiple data sources, directories, and/or metadirectories into a single view
- This avoids the overhead required associated with synchronization that a metadirectory requires
- Usually is a component of a larger IAM solution

All Rights Reserved, Continuum Worldwide, 2007

Federated Identity Management

- Tools and standards allow a user to use the same identity information among several companies or across domains
- Tools and standards allow trust relationships to be established to deal with identity information outside of a company's control
- May provide customers with inter-enterprise single sign-on, increasing traffic to web sites

All Rights Reserved, Continuum Worldwide, 2007

Federated Identity Management

- Security Assertion Markup Language (SAML)
  - User is locally authenticated
  - A security assertion is passed to the application via SAML
  - The application bases access controls on the security assertion provided
- Active Directory Federation Services (ADFS)
  - Extends Active Directory to the internet[1]
  - Based on WS-* architecture[1]
  - Supports SAML, Kerberos, and other tokens[1]

All Rights Reserved, Continuum Worldwide, 2007

User Provisioning

- New users may need access to a diverse array of resources.
  - E-mail
  - Network access
  - System access
- User provisioning tools can automatically add, modify, suspend, terminate user accounts for multiple resources
- Generally workflow processes are built in to user provisioning tools

All Rights Reserved, Continuum Worldwide, 2007

Authentication Technologies

- Enterprise Single Sign-On
- Web Access Management (WAM)
- Password Management
- Versatile Authentication Servers
- Service Account Password Management (SAPM)
- Contactless Chip Cards
- Emerging Biometrics for User Authentication

All Rights Reserved, Continuum Worldwide, 2007

Enterprise Single Sign-On

- User authenticates once and gains access to multiple resources
- Reduced sign-on a more accurate term,100% SSO is usually not achieved
- Generally modification to the target resources is not required[2]
- Some vendors now using screen scraping wizards to assist in setting up ESSO making the process easy and quick to implement
- Organizations with solid web/directory application strategies, should not need an ESSO solution.

All Rights Reserved, Continuum Worldwide, 2007

Web Access Management (WAM)

- Previously separate access and control mechanisms were being developed for each web application
- WAM provides centralized authentication, authorization, and auditing for web-delivered applications[2]
- Similar functionality to ESSO is provided, but WAM technologies scale better to large external populations[3]

All Rights Reserved, Continuum Worldwide, 2007

Web Access Management (WAM)

- An abstraction layer, or middleware, that supports internal and external web applications and portals[4]
- May provide identity administration, user provisioning, role management, federated identity management, or NAC integration[2]
- Integration with non-web based applications allows WAM to be a low-cost alternative to IAM suites[3]

All Rights Reserved, Continuum Worldwide, 2007

Password Management

- The automation of password resets via user self-service and the synchronizing of passwords across all integrated platforms and applications[2]
- Allows users to reset their own passwords instead of requiring help desk assistance
- Reduces costs related to user down time and password reset requirements of help desk personnel

All Rights Reserved, Continuum Worldwide, 2007

Service Account Password Management (SAPM)

- A SAPM product should include
  - Secure Password storage
  - Password Release
  - Password Updates
  - Auditing
  - An API for use of passwords by applications
- An alternative to SAPM is Kerberos, or another security token mechanism

All Rights Reserved, Continuum Worldwide, 2007

Service Account Password Management (SAPM)

- Eliminates the need to hard code passwords, or store password in text files for applications and service accounts
- Allows applications to retrieve passwords when required using and API (Application Programming Interface)
- Administrators and application programmers no longer need to know application or service account passwords

All Rights Reserved, Continuum Worldwide, 2007

Versatile Authentication Servers (VAS)

- High profile breaches are eroding consumer confidence in the protection of sensitive data in on-line transactions
- User name/password mechanisms are generally used for authentication
- The purpose of VAS is to provide the capability to allow stronger authentication mechanisms to be used based on the associated risk level of the information being protected

All Rights Reserved, Continuum Worldwide, 2007

Versatile Authentication Servers (VAS)

- Server that can support authentication using public-key credentials (PKC's) and one of the two industry-standard one-time password (OTP) authentication methods, look for vendors that allow plug-ins for third-party authentication methods[2]
  - OATH - Initiative for Open Authentication
  - HOTP – Hash OTP
  - EMV – Europay, MasterCard and Visa
  - CAP – Chip Authentication Program

All Rights Reserved, Continuum Worldwide, 2007

Contactless Chip Cards

- Proximity cards (ISO 14443)
  - Distance of .5 meters or less
  - Smart card
- Vicinity Cards (ISO 15693)
  - Distance of up to 1.5 meters
  - Smart card
- RFID Cards
  - Greater distance potential
  - Memory card
  - Used for building access or supply chain tracking

All Rights Reserved, Continuum Worldwide, 2007

Contactless Chip Cards

- Proximity and vicinity cards can be used as strong authentication mechanisms for system access
- Increasing use in hospitals with “walkaway” logoff for doctors
- Defcon Hacks against RFID/Proximity Cards
  - http://day%20.hackaday.com/2007/08/04/defcon-15-exploiting-authentication-systems/
  - http://www.hackaday.com/2005/05/07/proximity-card-spoofer/

All Rights Reserved, Continuum Worldwide, 2007

Emerging Biometrics/User Authentication

- **Skin Spectroscopy**
  Skin spectroscopy recognizes skin by its optical properties. The system uses a sensor to illuminate a small patch of skin with multiple wavelengths of visible and near-infrared light. The light is reflected back after being scattered in the skin and is then measured for each of the wavelengths. The system analyzes the reflectance variability of the various light frequencies as they pass through the skin.
  Because the optical signal is affected by chemical and other changes to the skin, skin spectroscopy also provides a sensitive and relatively easy way to confirm that a sample is living tissue.[5]

All Rights Reserved, Continuum Worldwide, 2007

Emerging Biometrics/User Authentication

- **Vein Pattern**
  - Subcutaneous infrared absorption patterns are recorded to produce distinctive identification templates.
  - The user places his hand under an imager, which takes an image of the back of the hand.
  - Main dorsal blood vessels have higher temperatures than the surrounding tissue, so they appear brighter in the image.
  - Vein patterns are separated from the background. Since blood vessels grow as people grow, only the shape and distribution of the veins is considered.

  Limitations:

  Dirty hands cannot easily be identified

  Not portable—or certainly less portable than other technologies.[5]

All Rights Reserved, Continuum Worldwide, 2007

Emerging Biometrics/User Authentication

- **Body Salinity**
  - Based on the natural level of salt in the human body.
  - Uses an electric field and salt's natural conductivity to measure an electrical current that is passed through the body.
  - This kind of biometric technology could include authentication of data transfer devices carried on the body, such as watches, mobile phones, and pagers. Also, applications could include "waking up" household appliances or devices as one enters a room. [5]

All Rights Reserved, Continuum Worldwide, 2007

Emerging Biometrics/User Authentication

- **Facial Thermography**
  - Based on the pattern of heat in the face caused by the flow of blood under the skin.
  - IR cameras capture this heat to produce a thermal pattern.

Limitations.

Dynamic nature of blood flow causes fluctuations and the appearance/disappearance of secondary patterns.

Environmental conditions (such as ambient temperature) and the introduction of alcohol or drugs, for example, can alter the thermal signature of the face.

Applications.

To determine “liveness” of the subject (no thermal image indicates no life)

Could indicate a rested or fatigued person or determine physical condition. [5]

All Rights Reserved, Continuum Worldwide, 2007

Authorization Technologies

- Enterprise Role Management
- Segregation of Duties Automation
- Network Access Control (NAC)/IAM Integration
- Automated Risk Analytics

All Rights Reserved, Continuum Worldwide, 2007

Enterprise Role Management

- Enterprises are noticing an issue with access creep due to a lack of central control over privileges
- Organizations are incorporating role based access controls to achieve efficiencies in access administration
- The purpose of enterprise role management solutions is to align IT access rights with business roles

All Rights Reserved, Continuum Worldwide, 2007

Enterprise Role Management

- Determining proper IT access rights for business roles is a difficult task for an enterprise
- Role engineering/mining products automate the process by managing, and reporting on entitlements of users by job function
- Each user may be assigned one or more roles
- Aids in user provisioning processes and maintaining entitlements

All Rights Reserved, Continuum Worldwide, 2007

Segregation of Duties Control

- Segregation of duties (SOD) controls are driven by regulatory compliance and security best practices
- These controls are in place to mitigate the risk of activities such as fraud and collusion
- Transaction monitoring is a good way to identify segregation of duties violations[1]
- An increasing number of ERP vendors providing SOD capabilities due to Sarbanes Oxley[1]

All Rights Reserved, Continuum Worldwide, 2007

Network Access Control (NAC)

- New focus due to higher risks
- Increasing number of mobile devices
- Unique challenges at the LAN
- Limit guest and visitor access with role-based network segmentation and VLAN defaulting

All Rights Reserved, Continuum Worldwide, 2007

Automated Risk Analytics

- Identity risk management, automates the process of identifying, measuring, and monitoring identity risk.
- Determine high risk accesses based on configurable algorithms – Risk Scoring
  - Critical systems and applications
  - Entitlements
  - Job function
  - Separation of Duties Violation

All Rights Reserved, Continuum Worldwide, 2007

Apocalypse of the Two Elephants

- Theory of standards by David Clark
- Similar to the Hype Cycle used by Gartner research to make recommendations on when to purchase a technology

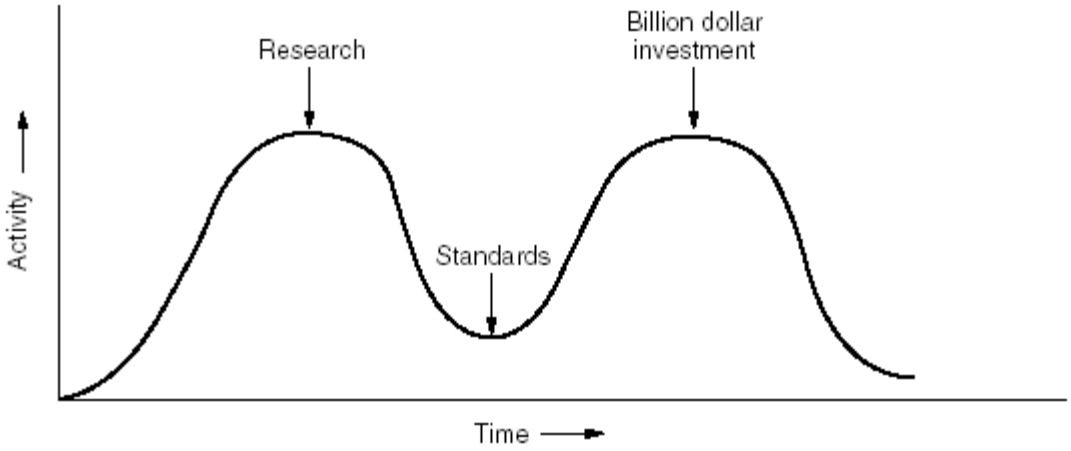

Figure 1-23. The apocalypse of the two elephants.

Tanenbaum, Andrew S. Computer Network Fourth Edition, Pearson Education, Inc. New Jersey 2003.

All Rights Reserved, Continuum Worldwide, 2007

Hype Cycle for IAM Technologies

Mature

- Enterprise Single Sign-On (ESSO)
- Web Access Management
- Password Management
- Metadirectories

Proven

- Segregation of Duties
- Federated Identity Management
- User Provisioning

Growing

- Contactless Chip Cards
- Service Account Password Management Tools (SAPM)
- Enterprise Role Management
- Virtual Directories

Emerging

- Emerging Biometric User Authentication
- Versatile Authentication Servers
- IAM/NAC Integration
- Automated Risk Analytics

All Rights Reserved, Continuum Worldwide, 2007

References

[1] Microsoft Corporation. (2004). Active Directory Federation Services: A Path to Federated Identity and Access Management.

[2] Kreizman, G., Enck, J., Litan, A., Wagner, R., Orans, L., Allan, A., MacDonald, N., Witty, R., Young, G., Ouellet, E., Runyon, B., Perkins, E. (2007). Hype Cycle for Identity and Access Management. Gartner

[3] Kirkdorffer, D., Gardiner, M. (2007). The Importance of Web Access Management Systems. *TechTarget Podcast Briefings.*

[4] Wagener, Ray. (2006). Magic Quadrant for Web Access Management, 2H06. Gartner.

[5] Ryan, Russ. (2006). Emerging Biometric Technologies. *SecurityInfowatch*.

All Rights Reserved, Continuum Worldwide, 2007