



Chapter XXIII

Identity Management: A Comprehensive Approach to Ensuring a Secure Network Infrastructure

Katherine M. Hollis, Electronic Data Systems, USA

David M. Hollis, United States Army, USA

Abstract

This chapter provides an introductory overview of identity management as it relates to data networking and enterprise information management systems. It looks at the strategic value of identity management in corporate and government environments. It defines the terms, concepts, and technologies associated with identity management. This chapter is a capstone to other chapters that deal with the specific technologies (strong identification and authentication, PKI, encryption, LDAP, etc...). Federated identity management is a strategic concept that encapsulates and integrates these disparate technologies into a coordinated, comprehensive strategy to accomplish enterprise-wide goals. This chapter introduces some practical business case concepts to assist the reader in putting together their own identity management strategies using ROI and success criteria.

Identity Management

Identity management (IdM) provides a combination of processes and technologies to securely manage and access the information and resources of an organization. IdM both protects and secures the organization and its information. It is a comprehensive approach that requires the integration of the entire network architecture — inherently providing an end-to-end solution.

With the widespread use of the Internet as a business-enabling platform, enterprises are seeing unprecedented opportunities to grow revenue, strengthen partnerships, achieve efficiencies, and win customer loyalty. The widespread use and openness of the Internet, which makes such communication in business relationships possible, also exposes core resources to corruption and inadvertent disruptions. An IdM strategy gives businesses a framework for protecting their infrastructure and incrementally addressing vulnerabilities while remaining open to new opportunities.

IdM is comprised of and supported by the full spectrum of network security technologies. IdM is the system of technologies and policies/procedures that allows the:

- identification,
- authentication,
- authorization,
- access control, and
- provisioning (secure repository)

of individuals, subsystems, objects, information, and data. It is intrinsic to the validation and secure manipulation of information and the control of individual users.

The integrity of an IdM system relies fundamentally on the validity and thoroughness of initial vetting procedures, to include identity management validity and strong authentication. This is intrinsic and provides the secure foundation for the entire infrastructure.

IdM systems technology consists of directory services, user provisioning and management, access management systems, and agents that monitor requests for resources and service. The foundation for a robust IdM system is the user data that typically resides in, preferably, a central store such as a directory server. Clean user data and well-defined business processes reduce the potential for data integrity issues and ensure that identity data across the enterprise is from an authoritative source. On this foundation is built the framework of rights and privileges that support IdM.

IdM, as noted above, is the amalgamation of business processes and technology that enable businesses, organizations, or government agencies to function as a single, secure, integrated entity with efficient, standardized processes for the management and maintenance of user rights and privileges. In an ideal world, each user possesses a single identity that can be leveraged across both the entire enterprise and an infrastructure that allows central management of users and access rights in an integrated, efficient and cost-effective way (EDS SPPS, 2004).

10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/identity-management-comprehensive-approach-ensuring/18399

Related Content

Competition and Coordination in a Dual-Channel Supply Chain With Asymmetric Retailers

YuHang Zhang and Ying Wang (2018). *International Journal of Enterprise Information Systems* (pp. 98-115).

www.irma-international.org/article/competition-and-coordination-in-a-dual-channel-supply-chain-with-asymmetric-retailers/203042

Identity Management: A Comprehensive Approach to Ensuring a Secure Network Infrastructure

Katherine M. Hollis and David M. Hollis (2006). *Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues* (pp. 372-383).

www.irma-international.org/chapter/identity-management-comprehensive-approach-ensuring/18399

Measuring the Impact of an ERP Project at SMEs: A Framework and Empirical Investigation

Maria Argyropoulou, George Ioannou, Dimitrios N. Koufopoulos and Jaideep Motwani (2009). *International Journal of Enterprise Information Systems* (pp. 1-13).

www.irma-international.org/article/measuring-impact-erp-project-smes/37197

Optimal Spectrum-Hole Detection Scheme for Cooperative CRN Using Dynamic Weighted VIKOR

Jayakumar Loganathan, S. Janakiraman and Ankur Dumka (2020). *International Journal of Enterprise Information Systems* (pp. 108-131).

www.irma-international.org/article/optimal-spectrum-hole-detection-scheme-for-cooperative-crn-using-dynamic-weighted-vikor/243706

An Optimal Missile Autopilot Design Model

Yong-chao Chen, Xin-bao Gao, Min Gao and Dan Fang (2018). *International Journal of Enterprise Information Systems* (pp. 104-110).

www.irma-international.org/article/an-optimal-missile-autopilot-design-model/198432