Identity Management:
Controlling Who’s Who in Your Network

Session SEC-150

What Is Identity Management?

Q. From which 1970s Rock and Roll Identity Mgmt. Classic came the lyrics...

“I woke up in a Soho doorway, a policeman knew my name”?

Identity Management Agenda

Identity Management Overview

Roadmap and Predictions

Technology Shifts

Identity Solutions

Who Are You?

- Enterprises need unified user control in the network (“AAA+A”)
  - Authenticate: recognize and verify user identity with digital mechanisms
  - Authorize: send policy and access control parameters for user access
  - Account (keep a record of user behavior/actions in network)
  - Address management and the ability to track and manage IP to ID mappings
Changing Network ID Dynamics

- Not just dial any longer...
  ISDN, Cable, DSL, VPN, Voice, Wireless, etc.
- Lowband to broadband
- Always on
- Public wires or airwaves
- Global availability, high scalability
- WAN/LANs merging

Identity Management Themes

- Expanding role of identity in your network
- Everything is changing:
  Scope, access type, complexity, global availability, security, scale, user types (employee, partner, contractor, etc.)
- Consolidation can help manage this increased complexity (identity tools, policies and user profiles)
Identity Management Agenda

Identity Management Overview

Roadmap and Predictions

Technology Shifts

Identity Solutions

Identity Technologies

• Three major trends:
  Stronger authentication
  Unification via directory
  New protocols, new demands on user-based policy
Identity Technologies—Authentication

“Strong authentication is the backbone to secure transactions. The User Authentication Market will double from $800 million in 2001 to $1.7 billion in 3 years.”


Identity Technologies—Authentication

• Three factors (three Ws)
  What you know (pin, password)
  What you have (token, keypair, smartcard)
  Who you are (fingerprint, voice, DNA…)

• “Two-factor” authentication is a common goal to increase security, better establish who your users are
Identity Technologies—Authentication

• Ways to authenticate to networks:
  
  Traditional username/password: (PPP, L2TP, PPTP, EAP-MD5CHAP, etc.)
  
  One-time passwords: (RSA SecurID, Secure Computing SafeWord, Cryptocard, Vasco, etc.)
  
  Public-key certificates and smartcards: (PKI vendors, Gemplus, Schlumberger...)
  
  Biometrics: (future)

How RSA Works

• Each user or device creates a “public” and “private” keypair; users prove their identity by “signing” packets with their private keys

1. Firewall sends a challenge phrase
2. Using her private key, Alice signs challenge phrase and returns response
3. Firewall verifies signature with Alice's public key, trusts that the keys belong to Alice by trusting the certificate
Public Keypairs as Identity Tools

- Public keypairs such as RSA can serve as “what you have” factor of authentication
- Digitally prove yourself by owning a set of keys that were exclusively belong to you
- Trust provided by certificates

Cisco Experience in PKI

- Benefits include:
  - Potentially Service Provider scalability
  - Well known, well studied security foundation of public-key cryptography
  - Increasing leverage across network, enterprise ID management systems

- Challenges include:
  - Immature standards
  - Evolving market: insource, outsource models
  - Considerable proprietary, scaling hurdles left
Weak vs. Strong Authentication

Source: Gartner Group, "Building Trust in Online Identities", 2001 p 3

Identity Technologies—Directories

Copyright © 1998, Cisco Systems, Inc. All rights reserved. Printed in USA.
Presentation_ID.scr
Identity Technologies—LDAP and DEN

- (Even) network identity components can be quite disparate
- Common directory models can help (DEN)

Identity Technologies—Directories

- User access control in particular can leverage a central, distributed directory service for user, group profile information
- A good start with LDAP
Identity Technologies—
Roles of Directory

• LDAP!= information models, schema still required
• User authentication, account administration, group membership information
• Storage of per-user/per-group authorization policies and profiles for network services
• Storage of ACS system config. info
• In a distributed environment, directory replication can provide global, logical views of such information

Benefits of LDAP User Model

• Manageability:
  “Single” strategic data source for all users
  Ability to replicate Identity service globally, in scale

• Information sharing:
  Key resource to manage various external configuration and user profile requirements
  Key ability to link network user with vertical (network) and horizontal (enterprise application) requirements for user profiles

• Scalability:
  Directory enables true, distributed, three-tiered architecture
Identity Technologies—User Policy

- Expanding networks need access type-aware user profiles networks
- At the same time, expanding networks need central interface to user management

Identity Technologies—User Policy

- What network resources can this user access/traverse?
- What security policies (key sizes, cert. attributes, IPsec SAs, etc.)?
- What times of day, for how long?
- How do we track/monitor user behavior?
- Varying requirements for enterprise and service provider management systems
- When resources are scarce, they need metering
Defining User Policies

- RADIUS and TACACS+ still the best game in town for AAA policy points
- Web access, SSO, PMI still evolving

Identity Management Agenda

Identity Management Overview
Roadmap and Predictions
Identity Solutions
Technology Shifts
Identity Management Tools at Cisco

- Expanding both broad-based user access control (RADIUS) and admin network access/config (TACACS+)
- Track and leverage existing and new Identity standards: DEN, DIAMETER, Kerberos, PKI, etc.
- Register, partition and track user services integrated with directories, provide more flexible and dynamic user policies
- Maintain close integration with DNS/DHCP

Identity Solutions

- Usage scenarios
  General
  802.1x LANs
  Wireless
User Access to the Network

- Global Office LAN - LAN VPN
- Remote Access Dialup and Roaming Users
- SP Gateway (Proxy AAA)
- VPN Gateways and Firewalls at Central Site
- Determines User Access Control Based on User Authentication, User Group Memberships in Directory

User LAN Security Management: 802.1x in a Nutshell

1. Switch ports designated to “uncontrolled”; only EAPOL authentication frames allowed
2. Client sends EAPOL authentication to switch
3. Switch forwards EAPOL via RADIUS request for user login to 802.1x enabled RADIUS server
4. RADIUS server responds with RADIUS accept/reject and (optional) VLAN ID info
5. Based on user credentials, access enabled or rejected for that port and (optionally) edge port configuration dynamically changed to new policy settings

Policy Table

<table>
<thead>
<tr>
<th>Login Name</th>
<th>VLAN</th>
<th>Access Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>joe</td>
<td>sales</td>
<td>M-F Day</td>
</tr>
<tr>
<td>bill</td>
<td>mktg</td>
<td>M-Sat.</td>
</tr>
<tr>
<td>mary</td>
<td>eng</td>
<td>Any</td>
</tr>
</tbody>
</table>

802.1x Switched LAN

Wiring Closet

Requires 802.1x Clients
User Identity 802.1x for Wireless

1. Wireless client initiates 802.1x user login to AP with EAPOL-Start packet
2. AP initiates RADIUS-Access-Request with RADIUS server
3. RADIUS server sends login challenge
4. Client logs in with username/pwd; AP sends response, server challenge to RADIUS
5. RADIUS server looks up user record either kept locally or via NT/AD domains, ODBC, LDAP
6.a RADIUS server uses MPPE to generate dynamic session key; Sends response to client via AP, including session key
6.b RADIUS server sends response to client via AP, including session key
7. Client authenticates server by comparing MPPE derived locally with MPPE keys returned from AP; Only valid RADIUS server with access to same user credentials will match. 802.1x access allowed

Identity Management Agenda

- Identity Management Overview
- Technology Shifts
- Roadmap and Predictions
- Identity Solutions
AAA Related Standards

- Kerberos
- RADIUS and TACACS+
- LDAP
- PKIX
- IEEE 802.1X
- Kerberos (again)
- DIAMETER

Cisco Identity Roadmap

<table>
<thead>
<tr>
<th>Historic</th>
<th>Access Control</th>
<th>PKI</th>
<th>LDAP</th>
<th>Policy</th>
<th>WAN/LAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS</td>
<td>None</td>
<td>PKCS</td>
<td>None</td>
<td>Limited</td>
<td>Primarily Dial-Up</td>
</tr>
<tr>
<td>RADIUS and TACACS+</td>
<td>Simple Cert. Enrollment Protocol (SCEP)</td>
<td>Authentication Lookups</td>
<td>Vendor Specific Attributes (VSAs)</td>
<td>Expanding Standards TBD</td>
<td>Many WANs</td>
</tr>
<tr>
<td>Future</td>
<td>DIAMETER</td>
<td>Full PKIX</td>
<td>Full LDAP User, Policy and Configs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WAN/LANs Merging</td>
</tr>
</tbody>
</table>
Roadmap

“I’d like to see Cisco specific efforts that bind the application/user level to the routed/IP level in a reasonably dynamic and manageable way.”

(Name Withheld, Major U.S. Bank)

My Industry Scorecard

<table>
<thead>
<tr>
<th>Service</th>
<th>Grade</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS/TACACS</td>
<td>A</td>
<td>Strong Vendor Interoperability; Vendor Extension Model Works</td>
</tr>
<tr>
<td>PKI and Stronger Authentication</td>
<td>C</td>
<td>Progress Is Slow</td>
</tr>
<tr>
<td>User Policy Standardization</td>
<td>C+</td>
<td>Web Vendors, Enterprise Applications and Network Vendors Need to Address Better Directory Unification of User Profiles</td>
</tr>
<tr>
<td>User Reporting/Auditing</td>
<td>B+</td>
<td>Up and Coming: Dedicated Solution Providers Focusing on User Reporting Problem</td>
</tr>
<tr>
<td>Security Integration</td>
<td>B</td>
<td>AAA Support Fairly Well Flushed through Network Access Gateway Solutions</td>
</tr>
<tr>
<td>User Handling</td>
<td>C+</td>
<td>No Per-User Granularity for QoS, DHCP, etc.</td>
</tr>
<tr>
<td>Mobility</td>
<td>B</td>
<td>DIAMETER Will Help</td>
</tr>
<tr>
<td>Scalability</td>
<td>B-</td>
<td>LDAP Will Help</td>
</tr>
<tr>
<td>Roadmap</td>
<td>A</td>
<td>;</td>
</tr>
</tbody>
</table>
Roadmap

“Once, it was sufficient to protect the perimeter. Keeping people out was more important than letting them in, but times have changed. The 3As enable enterprises to open their internal networks to external access via the Internet.”


Thank You
Identity Management: Controlling Who’s Who in Your Network

Session SEC-150

Please Complete Your Evaluation Form

Session SEC-150