Lesson 8

Implementing Identity and Account Management Controls

CompTIA

Topic 8A

Implement Identity and Account Types

Syllabus Objectives Covered

- 3.7 Given a scenario, implement identity and account management controls
- 5.3 Explain the importance of policies to organizational security

Identity Management Controls

- Certificates and smart cards
  - Public key cryptography
  - Subject identified by a public key, wrapped in digital certificate
  - Private key must be kept secure
- Tokens
  - Authorizations issued under single sign-on
  - Avoids need for user to authenticate to each service
- Identity provider
  - Provisions and manages accounts
  - Processes authentication
  - Federated identity management

Background Check and Onboarding Policies

- Human resources (HR) and personnel policies
  - Recruitment (hiring)
  - Operation (working)
  - Termination/separation (firing or retiring)
- Background check
- Onboarding
  - Welcoming a new employees or contractors to the organization
  - Account provisioning
  - Issuing credentials
  - Asset allocation
  - Training/policies
- Non-disclosure Agreement (NDA)

Personnel Policies for Privilege Management

- Mitigate insider threat
- Separation of duties
  - Standard operating procedures (SOPs)
  - Shared authority
- Least privilege
  - Assign sufficient permissions only
  - Reduce risk from compromised accounts
- Job rotation
  - Distributes institutional knowledge and expertise
  - Reduces critical dependencies
- Mandatory vacations

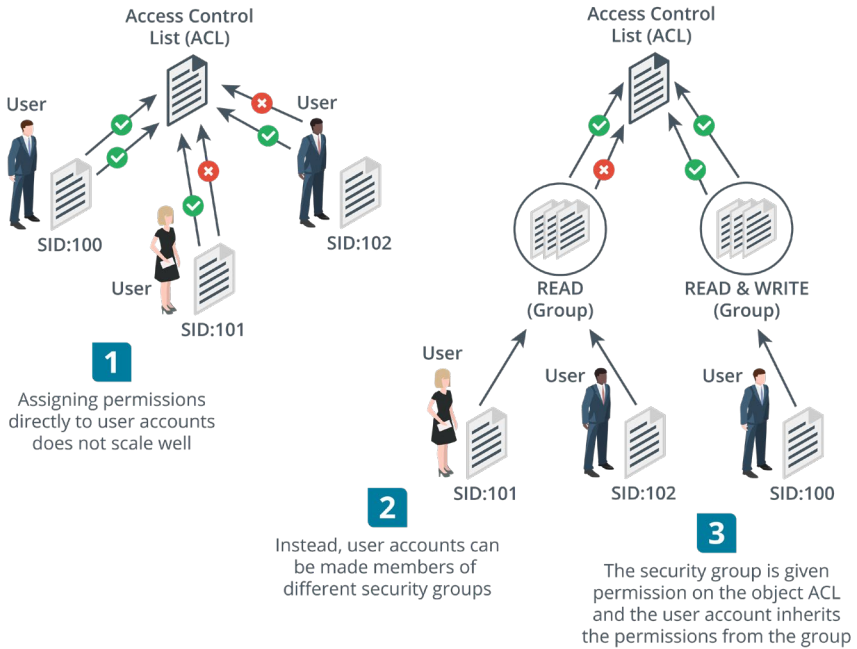
Offboarding Policies

- Identity and access management checks
  - Disable the user account and privileges
  - Ensure integrity and availability of information assets managed by the employee
- Retrieving company assets
- Returning personal assets
- Consider shared/generic accounts, security procedures that must be changed

Security Account Types and Credential Management

- Standard users
  - Limited privileges
  - Should not be able to change the system configuration
  - Restricted to account profile
- Credential management policies for personnel
  - Password policy
  - Protect access to the account and prevent compromise
  - Educate risks from reusing credentials and social engineering
- Guest accounts
  - Account with no credentials (anonymous logon)
  - Unauthenticated access to hosts and websites
  - Must have very limited privileges or be disabled

Security Group-Based Privileges



- User-assigned privileges
  - Assign privileges directly to user accounts
  - Unmanageable if number of users is large
- Group-based privileges
  - Assign permissions to security groups and assign user accounts to relevant groups
  - Issues with users inheriting multiple permissions

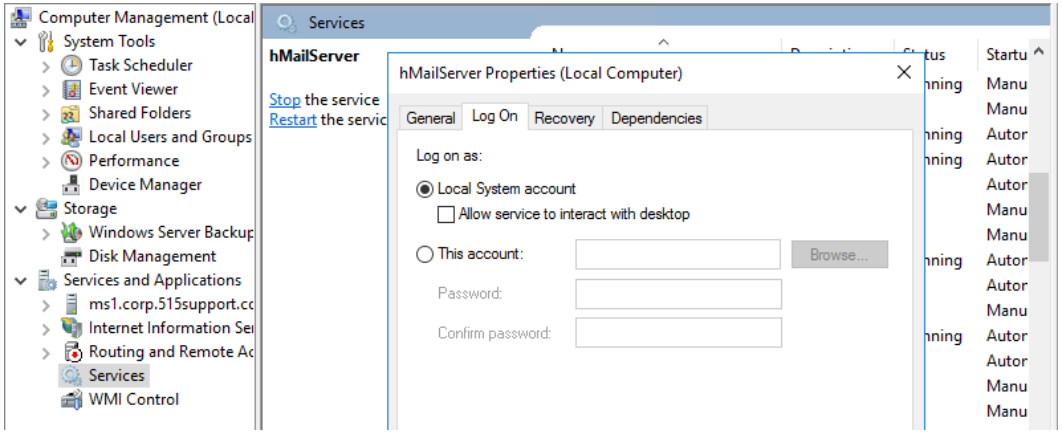
Images © 123RF.com.

Administrator/Root Accounts

- Privileged/administrative accounts
  - Can change system configuration
- Generic administrator/root/superuser
  - User account with full control over system
  - Key target for attackers
  - Often disabled or usage restricted after install
- Administrator credential policies
  - Create specific accounts with least privileges (generic account prohibition)
  - Enforce multifactor authentication
- Default security groups
  - Administrators/sudoers

Service Accounts

- Windows service accounts
  - System
  - Local Service
  - Network Service
- Linux accounts to run services (daemons)
  - Deny shell access
- Managing shared service account credentials

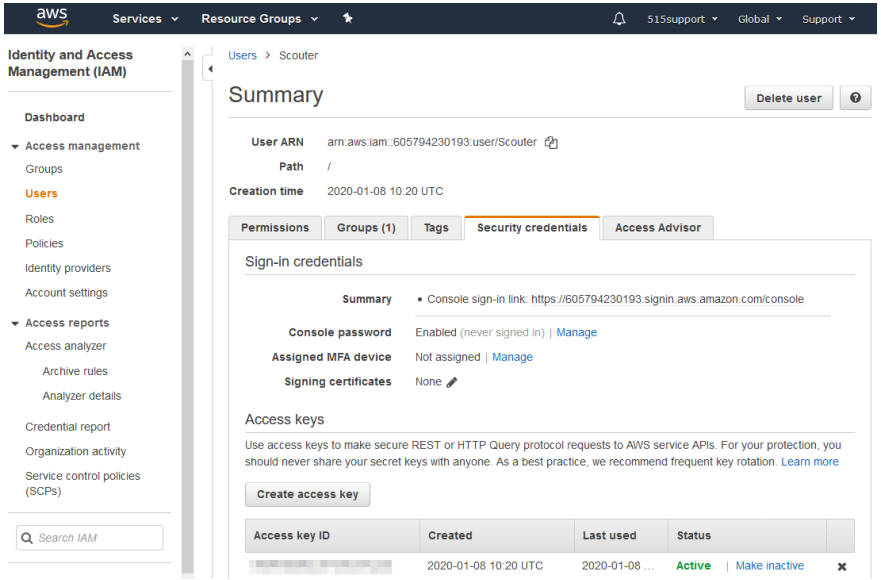


Screenshot used with permission from Microsoft.

Shared/Generic/Device Accounts and Credentials

- Shared accounts
  - Accounts whose credentials are known to more than one person
- Generic accounts
  - Accounts created by default on OS install
  - Only account available to manage a device
  - Might use a default password
- Risks from shared and generic accounts
  - Breaks principle of non-repudiation
  - Difficult to keep credential secure
- Credential policies for devices
- Privilege access management software

Secure Shell Keys and Third-party Credentials



Screenshot used with permission from Amazon.com.

- Secure Shell (SSH) used for remote access
  - Host key identifies the server
  - User key pair used to authenticate to server
  - Server holds copy of valid users' public keys
  - Keys must be actively managed
- Third-party credentials
  - Passwords and keys to manage cloud services
  - Highly vulnerable to accidental disclosure

Topic 8B

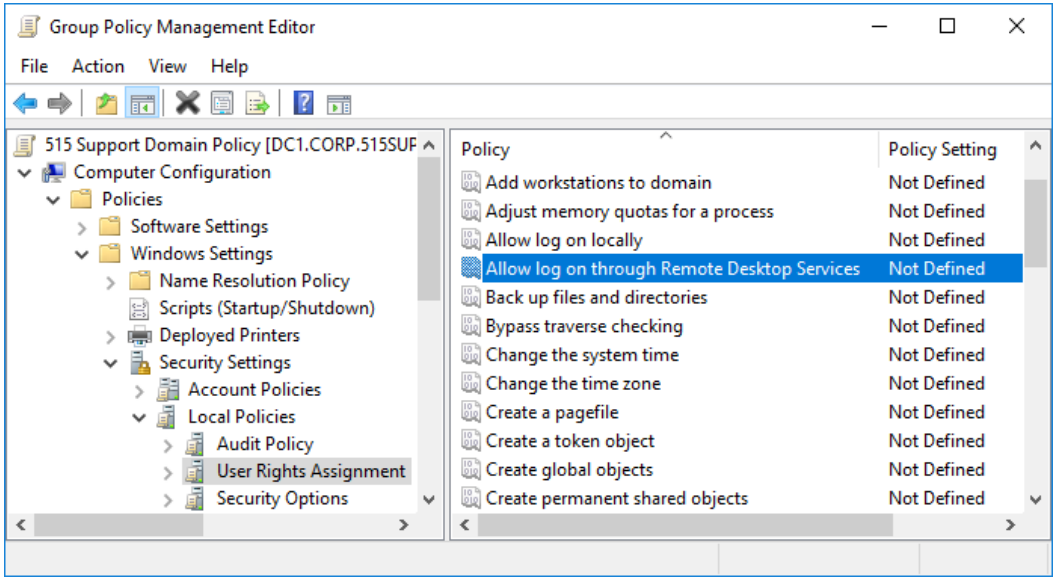
Implement Account Policies

Syllabus Objectives Covered

- 3.7 Given a scenario, implement identity and account management controls

Account Attributes and Access Policies

- Account attributes
  - Security ID, account name, credential
  - Extended profile attributes
  - Per-app settings and files
- Access policies
  - File permissions
  - Access rights
  - Active Directory Group Policy Objects (GPOs)



Screenshot used with permission from Microsoft.

Account Password Policy Settings

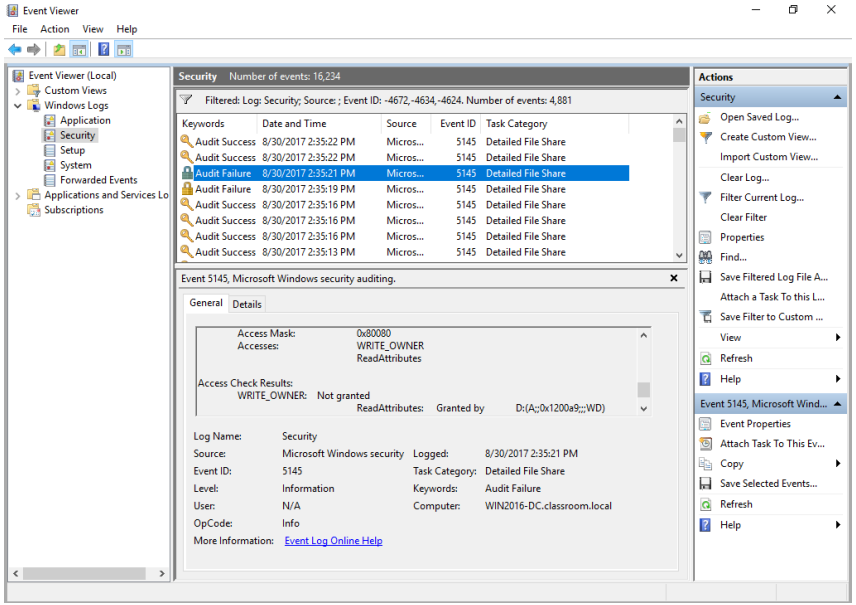
- Length
- Complexity
  - Character combinations
- Aging
- History and reuse
- NIST guidance
- Password hints

Account Restrictions

- Network location
  - Connecting from a VLAN or IP subnet/remote IP
  - Connecting to a machine type or group (clients versus servers)
  - Interactive versus remote logon
- Geolocation
  - By IP address
  - By Location Services
  - Geofencing
  - Geotagging
- Time-based restrictions
  - Logon hours
  - Logon duration
  - Impossible travel time/risky login

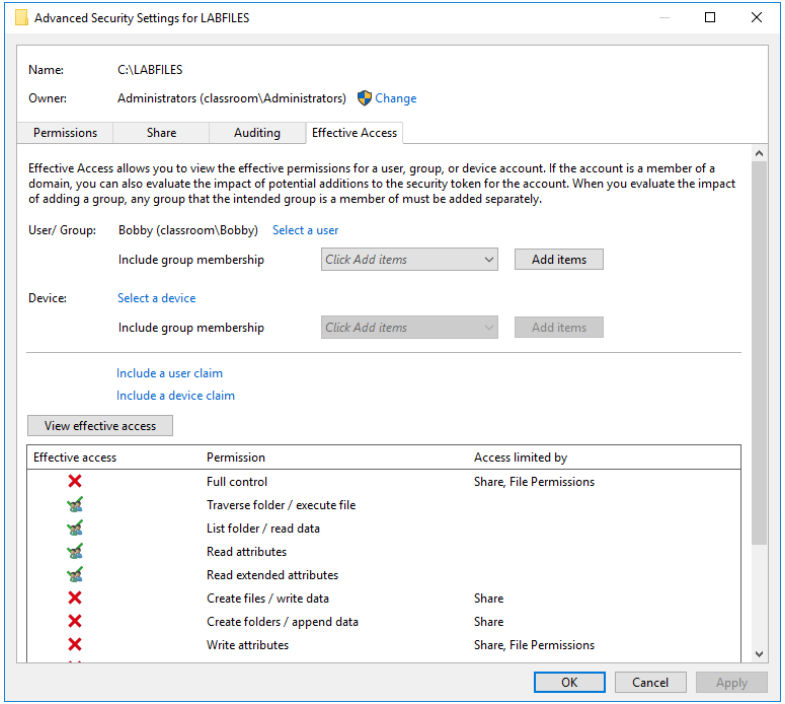
Account Audits

- Accounting and auditing to detect account misuse
  - Use of file permissions to read and modify data
  - Failed login or resource access attempts
- Recertification
  - Monitoring use of privileges
  - Granting/revoking privileges
  - Communication between IT and HR



Screenshot used with permission from Microsoft.

Account Permissions

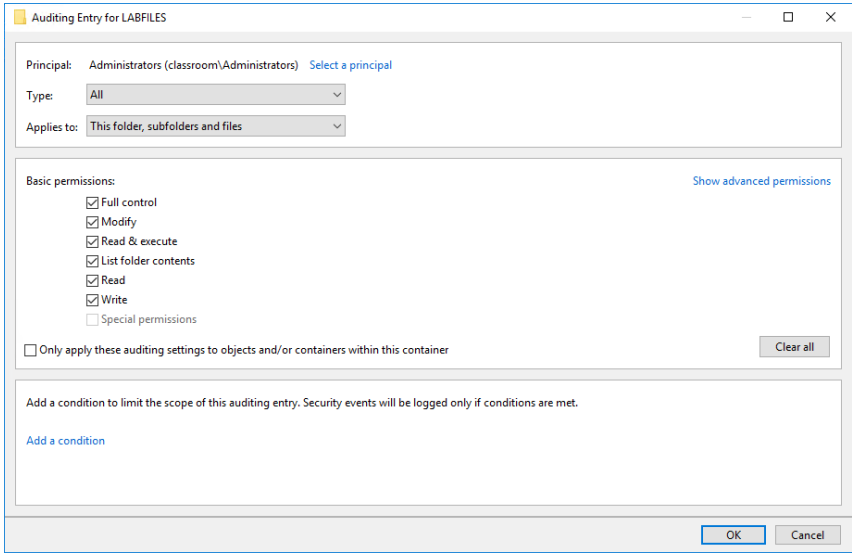


Screenshot used with permission from Microsoft.

- Impact of improperly configured accounts
  - Insufficient permissions
  - Unnecessary permissions
- Escalating and revoking privileges
- Permission auditing tools

Usage Audits

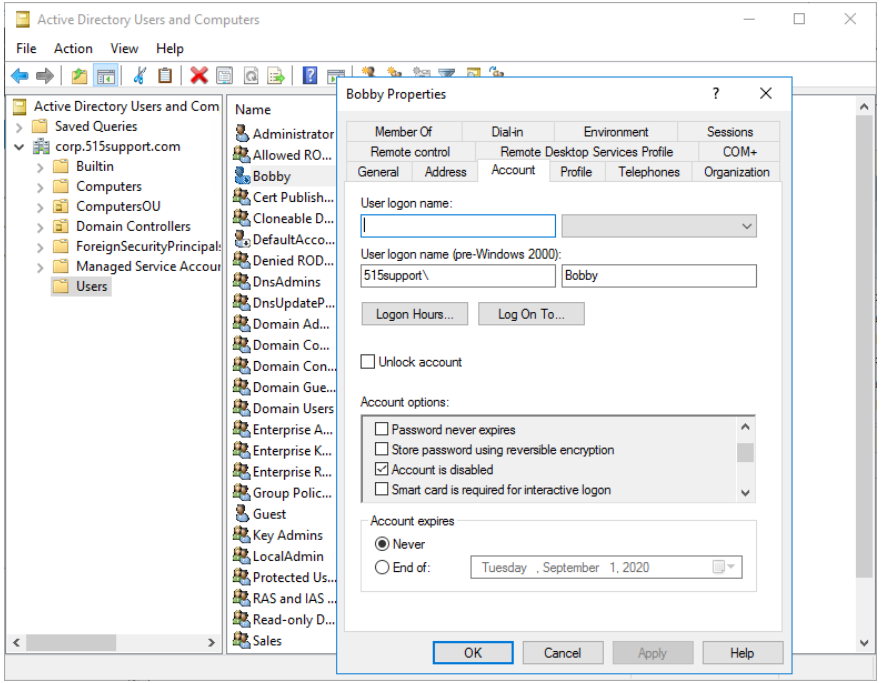
- Account logon and management events
- Process creation
- Object access (file system / file shares)
- Changes to audit policy
- Changes to system security and integrity (anti-virus, host firewall, and so on)



Screenshot used with permission from Microsoft.

Account Lockout and Disablement

Screenshot used with permission from Microsoft.



- Disablement
  - Login is disabled until manually re-enabled
  - Combine with remote logoff
- Lockout
  - Login is prevented for a period and then re-enabled
  - Policies to enforce automatic lockout

Topic 8C

Implement Authorization Solutions

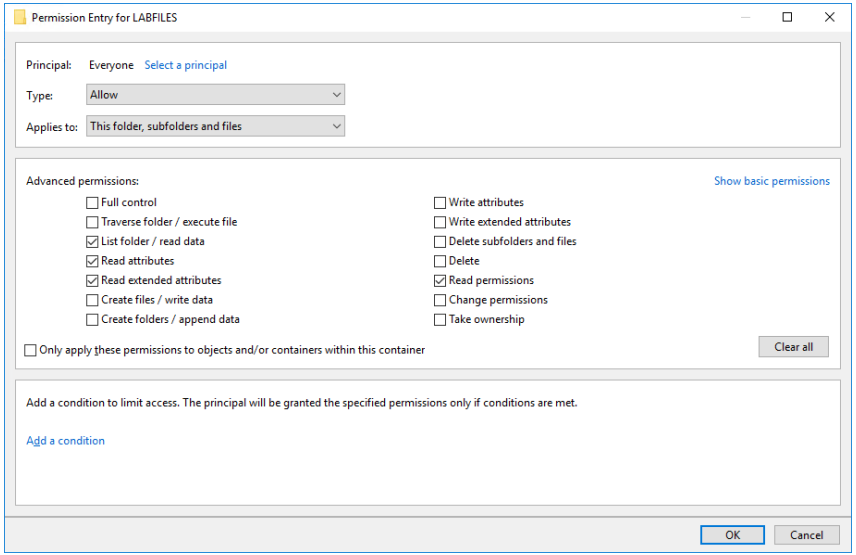
Syllabus Objectives Covered

- 2.4 Summarize authentication and authorization design concepts
- 3.8 Given a scenario, implement authentication and authorization solutions
- 4.1 Given a scenario, use the appropriate tool to assess organizational security (chmod only)

Discretionary and Role-Based Access Control

- Access control model determines how users receive permissions/rights
- Discretionary Access Control (DAC)
  - Based on resource ownership
  - Access Control Lists (ACLs)
  - Vulnerable to compromised privileged user accounts
- Role-Based Access Control (RBAC)
  - Non-discretionary and more centralized control
  - Based on defining roles then allocating users to roles
  - Users should only inherit role permissions to perform particular tasks

File System Security



Screenshot used with permission from Microsoft.

- Access Control List (ACL)
- Access Control Entry (ACE)
- File system support
- Linux permissions and chmod
  - Symbolic (rwx)
  - User, group, world
  - Octal
    - r=4
    - w=2
    - x=1

Mandatory and Attribute-Based Access Control

- Mandatory Access Control (MAC)
  - Labels and clearance
  - System policies to restrict access
- Attribute-Based Access Control (ABAC)
  - Access decisions based on a combination of subject and object attributes plus any context-sensitive or system-wide attributes
  - Conditional access

Rule-Based Access Control

- Non-discretionary
  - System determines rules, not users
- Conditional access
  - Continual authentication
  - User account control (UAC)
- Privileged access management
  - Policies, procedures, and technical controls to prevent the malicious abuse of privileged accounts

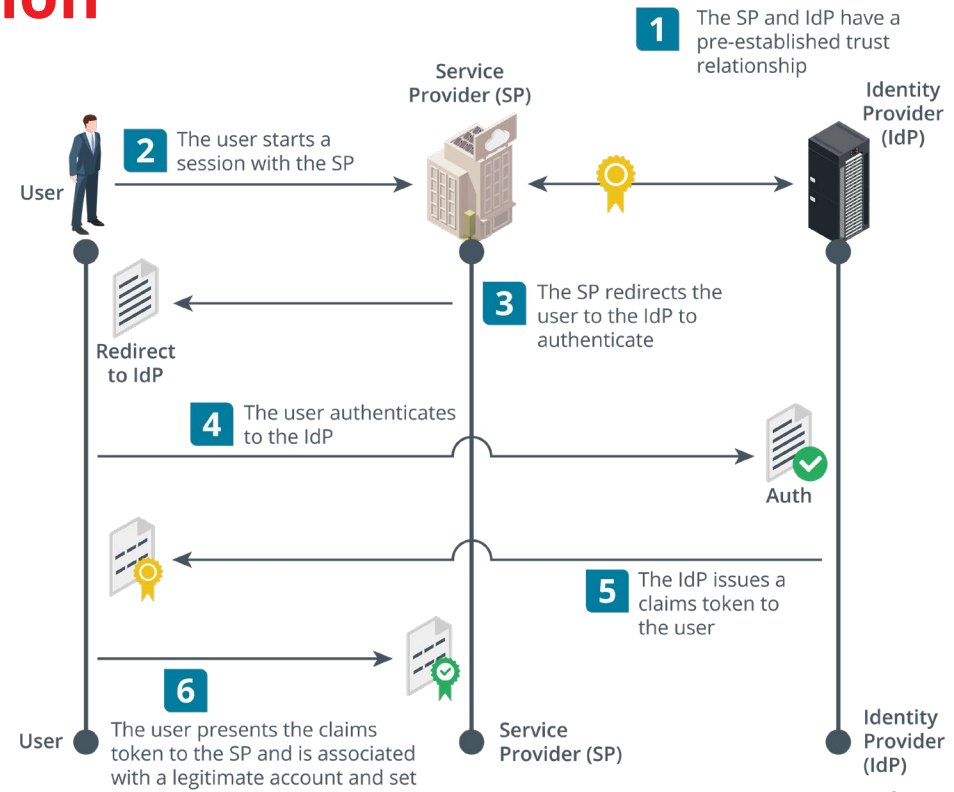
Directory Services

- Database of subjects
  - Users, computers, security groups/roles, and services
- Access Control Lists (authorizations)
- X.500 and Lightweight Directory Access Protocol (LDAP)
  - Distinguished names
  - Attribute=Value pairs

CN=WIDGETWEB, OU=Marketing, O=Widget, C=UK, DC=widget, DC=foo

Federation and Attestation

- Federated identity management
  - Networks under separate administrative control share users
- Identity providers and attestation
- Cloud versus on-premises requirements



Images © 123rf.com.

Security Assertions Markup Language

- Open standard for implementing identity and service provider communications
- Attestations/assertions
  - XML format
  - Signed using XML signature specification
- Communications protocols
  - HTTPS
  - Simple Object Access Protocol (SOAP)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="200"
Version="2.0"
IssueInstant="2020-01-01T20:00:10Z"
Destination="https://sp.foo/saml/acs" InResponseTo="100".
  <saml:Issuer>https://idp.foo/sso</saml:Issuer>
  <ds:Signature>...</ds:Signature>
  <samlp:Status>...(success)...</samlp:Status.
<saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="2000" Version="2.0"
IssueInstant="2020-01-01T20:00:09Z">
<saml:Issuer>https://idp.foo/sso</saml:Issuer>
<ds:Signature>...</ds:Signature>
   <saml:Subject>...
   <saml:Conditions>...
    <saml:AudienceRestriction>...
    <saml:AuthnStatement>...
    <saml:AttributeStatement>
        <saml:Attribute>...
        <saml:Attribute>...
    </saml:AttributeStatement>
   </saml:Assertion>
</samlp:Response>
```

OAuth and OpenID Connect

- "User-centric" federated services better suited to consumer websites
  - Representational State Transfer (REST) Application Programming Interfaces (APIs) (RESTful APIs)
  - Framework for implementation not a protocol
- OAuth
  - Designed to communicate authorizations rather than explicitly authenticate a subject
  - Client sites and apps interact with OAuth IdPs and resource servers that hold the principal's account/data
  - Different flow types for server to server or mobile app to server
  - JavaScript object notation (JSON) web token (JWT)
- OpenID Connect (OIDC)
  - Adds functions and flows to OAuth to support explicit authentication

Topic 8D

Explain the Importance of Personnel Policies

Syllabus Objectives Covered

- 5.3 Explain the importance of policies to organizational security

Conduct Policies

- Acceptable use policy (AUP)
  - Employee use of employer's hardware and software assets
- Rules of behavior and social media analysis
  - General requirements for professional standards
  - Covers personal communications and social media accounts
  - Additional clauses for privileged users
- Use of personally owned devices
  - Bring your own device
  - Shadow IT
- Clean desk

User and Role-based Training

- Impacts and risks from untrained users
- Topics for security awareness
  - Overview of security policies
  - Incident response procedures
  - Site security procedures
  - Data handling
  - Password and account management
  - Awareness of social engineering and malware threats
  - Secure use of software such as browsers and email clients
- Role-based training
  - Appropriate language
  - Level of technical content

Diversity of Training Techniques

- Engagement and retention
- Training delivery methods
- Phishing campaigns
  - Simulating phishing messages to test employee awareness
- Capture the flag
- Computer-based training (CBT)
  - Simulations
  - Branching scenarios
  - Gamification elements

Lesson 8

Summary