

Domain 5: Identity & Access Management

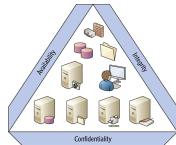
MIS-5903

<https://community.mis.temple.edu/mis5903sec711summer2021/>

1

Security Principles – Availability

- Information accessible in a timely manner, so productivity not adversely affected
- Fault tolerance and recovery mechanism ensure continuity of the availability of resources
- Attributes:
 - Accuracy
 - Relevance
 - Timeliness
 - Privacy



6/15/21

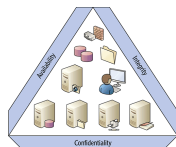
MIS5903 – Domain 5

2

2

Security Principles – Integrity

- Information must be:
 - Accurate
 - Complete
- Protected from unauthorized modification
- Protects data, or a resource, from being altered in an unauthorized fashion



6/15/21

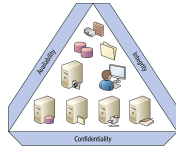
MIS5903 – Domain 5

3

3

Security Principles – Confidentiality

- Information not disclosed to unauthorized
 - Individuals
 - Programs
 - Processes
- Security Mechanisms:
 - Encryption
 - Logical and Physical access controls
 - Transmission protocols
 - Database Views
 - Controlled traffic flow
 - VPN, IPSec



6/15/21

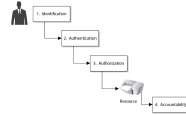
MS5903 – Domain 5

4

4

Four Steps to Access an Object

- Identification
 - Subjects supply identification information
 - Username, User ID, account number
- Authentication
 - Verifying the identification information
 - Passphrase, PIN Value, thumbprint, smart card, one-time password
- Authorization
 - Using identity of subject with other criteria to determine authorized actions
 - "I know who you are, now what can you do?"
- Accountability
 - Audit logs and monitoring to track subject <-> object interaction attempt(s)



6/15/21

MS5903 – Domain 5

5

5

Identity Management - Identification

- Identification should be:
 - Unique, for user accountability
 - Standard naming scheme
 - Non-descriptive of position or tasks
 - Not shared between users
- Identity Management (IdM)
- Identity and Access Management (IAM)

6/15/21

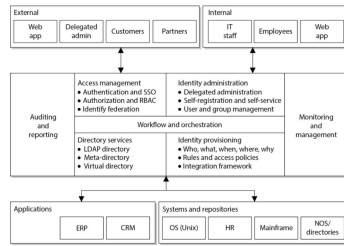
MS5903 – Domain 5

6

6

Access Concerns

- What resources?
- Who approves?
- Maps to policies?
- Access Revocation?
- Access Review
- Compliance with
 - Regulations
 - Contracts
 - Organizational policies



6/15/21

MIS5903 - Domain 5

7

7

Directories

- X.500, LDAP, Active Directory
- DN: cn=First Last, dc=temple, dc=edu
- Tree structure to organize entries using parent-child
- Attributes dictated by defined schema
- Unique identifiers are called distinguished names
- Subtrees for service, agency, department, etc.

6/15/21

MIS5903 - Domain 5

8

8

Web Access Management (WAM)

- User sends credentials to web server
- Web server requests WAM platform to authenticate user (against LDAP)
- User (subject) requests access to object
- Web server verifies object access is authorized, and allows access to resource/object

6/15/21

MIS5903 - Domain 5

9

9

Password Management

- Password synchronization
- Self-service password reset
- Assisted password reset
- Legacy Single Sign On (SSO)

6/15/21

MIS5903 - Domain 5

10

10

Accounts

- Account Management
- Registration
- Provisioning
 - Identity Provisioning
- Authoritative System of Record
- Profile Update

6/15/21

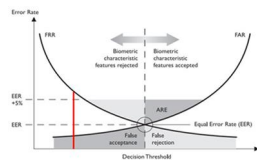
MIS5903 - Domain 5

11

11

Biometrics

- Physiological – “what you are”
- Behavioral – “what you do”
- Accuracy:
 - Type 1 error – False Rejection Rate (FRR)
 - Type 2 error – False Acceptance Rate (FAR)
 - Crossover Error Rate (CER)



6/15/21

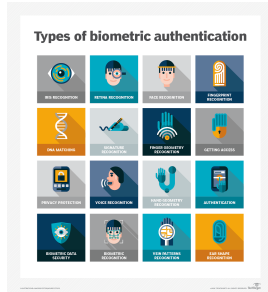
MIS5903 - Domain 5

12

12

Biometric Methods

- Fingerprint
- Palm Scan
- Hand Geometry
- Retina Scan
- Iris Scan
- Signature Dynamics



6/15/21 MISS903 - Domain 5 13

13

Passwords

- Password Policies – Length, Complexity, Frequency, History, Limit Logon Attempts
- Clipping Level
- Cognitive Password – fact or opinion-based information
 - CAPTCHA
- One Time Password (token, smartphone)
 - Synchronous – uses time or a counter as a core piece of authentication
 - Counter-synchronization – user triggered
 - Asynchronous – authentication server sends a challenge (“nonce”); token encrypts and sends the result to server
- Passphrase – sequence of characters longer than a password.

6/15/21 MISS903 - Domain 5 14

14

Password Attacks

- Electronic monitoring
- Access the password file
- Brute Force Attacks
- Dictionary Attacks
- Social Engineering
- Rainbow Table (pre-calculated hash values)

- Password checker used by a security professional...
- Becomes a Password Cracker when used by hacker.

6/15/21 MISS903 - Domain 5 15

15

Password Hashing

- Commonly MD4 or MD5
- Salts are random values added for complexity and randomness
- Unix/Linux – “shadow”

6/15/21

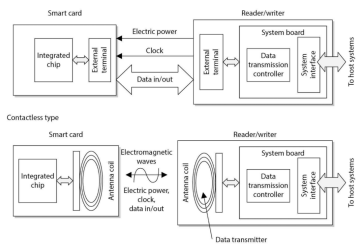
MS5903 – Domain 5

16

16

Cards

- Radio Frequency Identification (RFID)
- Memory cards – hold information, but cannot process information
- Smart card – process information (e.g. add PIN)



6/15/21

MS5903 – Domain 5

17

17

Access Card Attacks

- Fault Generation
- Side Channel Attacks – nonintrusive
 - Differential power analysis
 - Electromagnetic analysis
 - Timing
 - Software attacks

6/15/21

MS5903 – Domain 5

18

18

Authorization

- Access Criteria
 - Roles
 - Groups
 - Physical or Logical Location
 - Time of Day
 - Temporal
 - Transaction Type (e.g. upper limit)
- Default to No Access
- Need to Know
- Beware of Authorization Creep over time

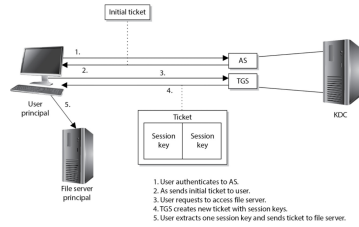
6/15/21

MIS5903 - Domain 5

19

19

Kerberos



6/15/21

MIS5903 - Domain 5

20

20

Kerberos Weaknesses

- If one KDC < Single Point of Failure
- Must be scalable, able to handle requests
- Secret keys store on user workstations temporarily
- Session keys decrypted and reside in cache or key table
- Vulnerable to password guessing.
- Must enable encryption. (not on by default)
- If keys too short, can be brute-force attacked
- Clocks must be synchronized

6/15/21

MIS5903 - Domain 5

21

21

Security Domain

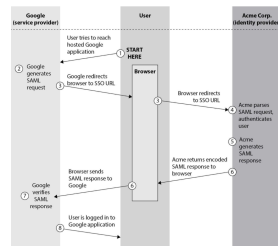
- Resources available to a subject
- Resources within the same logical structure (domain) work under the same security policy and are managed by the same group
- Federation – authenticate to Company A, Assertion authenticates to secondary company. (Federated Identity)
- Thin Clients – relies upon central server for access control, processing, and storage

6/15/21 MISS903 – Domain 5 22

22

Access Control & Markup Languages - SAML

- Security Assertion Markup Language (SAML) - exchange between domains
 - User = principal
 - Cloud Provider = Service Provider
 - Organization = Identity Provider

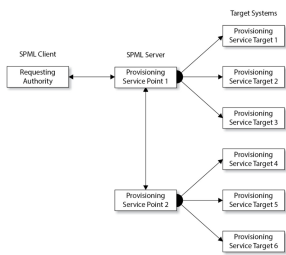


6/15/21 MISS903 – Domain 5 23

23

Access Control & Markup Languages (2) - SPML

- Requesting Authority (RA)
- Provisioning Service Provider (PSP)
- Provisioning Service Target (PST) - target



6/15/21 MISS903 – Domain 5 24

24

Access Control & Markup Languages (3)

- Extensible Markup Language (XML)
- Web Services = Service Oriented Architecture
- Simple Object Access Protocol (SOAP)
- SAML requests send within SOAP
- Extensible Access Control Markup Language (XACML)
 - Express security policies and access rights to assets provided through web services and other enterprise application
 - Subject element (requesting entity)
 - Resource element (requested entity)
 - Action element (types of access)

6/15/21

MIS5903 - Domain 5

25

25

Third Party Authentication/Authorization

- OpenID – open standard for user authentication by third parties
 - End User – wants to be authenticated
 - Resource user – server owns the resource
 - OpenID provider – system where the user already has an account.
- OAuth – open standard for authorization
 - Example – authorize one web site to access content on another site
- Identity as a Service (IDaaS)
 - SaaS offering that provides SSO, federated IdM, password management.
- Integration – in-house (all on site) or outsourced (some or all off-site)

6/15/21

MIS5903 - Domain 5

26

26

Access Control Models

- Discretionary Access Control (DAC) – data owner assigns ACLs
 - Identity Based – user or group
- Mandatory Access Control (MAC) – operating system refers to security labels
- Role Based Access Control (RBAC) – access based on subject’s role and/or functional position
 - Task Based Access Control (TBAC) – based on tasks assigned to the subject.
- Rule-based Access Control (RB-RBAC) – Adds on rules that further restrict access
- Attribute-Based Access Control – use of attributes (software-defined network) e.g “Allow Managers to access the WAN using mobile”

6/15/21

MIS5903 - Domain 5

27

27

Access Control Techniques & Technologies

- Access Control Lists (ACLs)
- Access Control Matrix (DAC) – object shows subjects and privileges
- Capability Table – what objects can (token, ticket, key) be access?
- Constrained User Interface
- Context Dependent Access Control (filter based on sensitivity)
- Context-Dependent Access Control

6/15/21

MS5903 – Domain 5

28

28

Centralized Access Control Administration

- Remote Authentication Dial-In User Service (RADIUS) – AAA
 - Uses TCP
 - Only password is encrypted
 - Attribute-Value Pairs
- Terminal Access Controller Access Control System (TACACS)
 - Uses UDP
 - Encrypts all traffic
 - Separates Authentication, Authorization, Auditing
 - Supports other protocols
 - Can define ACLs, filters, user privileges, more.
- Diameter – Base + Extensions

6/15/21

MS5903 – Domain 5

29

29

Access Control – Administrative

- Policy and procedures
- Personnel controls
- Supervisory structure
- Security awareness training
- Testing

6/15/21

MS5903 – Domain 5

30

30

Access Control – Physical

- Network segregation
- Perimeter security
- Computer controls
- Work area separation
- Data backups
- Cabling
- Control Zone – based on sensitivity

6/15/21 MIS5903 – Domain 5 31

31

Access Control – Technical

- System access
- Network architecture
- Network access
- Encryption and protocols
- Auditing

6/15/21 MIS5903 – Domain 5 32

32

Accountability – System Level

- Performance
- Logon attempts (successful and unsuccessful)
- Logon ID, Date & Time details
- Lockouts of users and terminals
- Use of Administrative utilities
- Devices used
- Functions performed
- Requests to alter configuration files

6/15/21 MIS5903 – Domain 5 33

33

Accountability – App/User Events

- Application-Level Events
 - Error messages
 - Files opened and/or closed
 - Modifications of files
 - Security violations within applications
- User-level events
 - Identification and authentication attempts
 - Files, services, resources used
 - Commands initiated
 - Security violations

6/15/21 MIS5903 – Domain 5 34

34

Review of Audit Information

- Audit retention
- Security Event Management (SEM)
- Security Information and Event Management (SIEM)
- Logs must be protected
- Keystroke Monitoring – be mindful of privacy issues

6/15/21 MIS5903 – Domain 5 35

35

Access Control Practices

- Deny undefined or anonymous accounts
- Limit and monitor privileged/powerful accounts
- Suspend or delay access after unsuccessful logon attempts
- Remove obsolete user accounts on departure
- Suspend inactive accounts after 30 to 60 days
- Enforce strict access criteria
- Enforce the need-to-know and least privilege
- Disable unneeded system features, services, ports

6/15/21 MIS5903 – Domain 5 36

36

Access Control Practices (2)

- Replace default password settings
- Limit and monitor global access rules
- Remove redundant resource rules from accounts and/or group memberships
- Remove redundant user IDs, accounts, role-based accounts from ACLs.
- Enforce password requirements: rotation, length, contents, lifetime, distribution, storage, transmission
- Audit System and user events and actions; review reports periodically
Protect audit logs

6/15/21

MIS5903 - Domain 5

37

37

Unauthorized Disclosure

- Object Reuse (USB drives, etc.)
- Emanation Security
 - TEMPEST
 - White Noise
 - Control Zone
- IDS/IPS
- Honeypot – “sacrificial lamb”
 - Line between enticement and entrapment
 - Distracts attacker from bastion hosts (DMZ hosts unprotected by firewalls/routers)

6/15/21

MIS5903 - Domain 5

38

38

Next Steps...

- Continue Discussion on Class Website
- Mid-Term
 - Expect 120 questions (120 questions = 180 minutes in one sitting)
 - First four domains
- Questions

6/15/21

MIS5903 - Domain 5

39

39