Security Architecture
- Week 4 -

Identity and Access Management

Week 4

- Week 3 Quiz
- Topics in-the-news
- Review of Week 3
- Week 4 Assignment
- Week 4 Lecture:
  - Identity and Access Management
- Quiz

Identity and Access Management

The ability to verify an individual's identity and, on that basis, restrict the facilities and resources to which they are privileged

Identity and Access Management

- Taking on more importance
- Used to be, principally, the process of managing user IDs and passwords
- Integrated network permissioning and single sign-on capabilities have made management processes essential
- Questions about the sufficiency of perimeter security have highlighted importance
- The multitude of devices, including personal devices, on the business network creates new needs
- Internet-of-things will complicate and magnify the impact

Passwords and Password Management

- Identity verification
- Password standards
- Power of awareness
- Moving beyond passwords

Identity Verification

- One ID for all activities
- Problem: how do you do this across different technologies
- The power of role-based privileging

Password Standards

- Renewal timing
  - 2 month is best practice
  - 3 month observed
- Complexity standards and enforcement
- Personal password management
- The password paradox
  - The more complex the password the more likely to:
    - Write it down
    - Use the same password for everything

The Power of Awareness

- Cost Effective Approach approach
- Protects against more than just ID related risks
- Encourages everyone to participate and take responsibility
- Can be an early warning and event escalation system if integrated with formal SIEM

Moving Beyond Passwords

- Basis for individual identification
  - something you know
  - something you have
  - something you are
- Variations of the password idea
  - Pass phrase
- Multi-factor authentication
  - Token device
  - Phone
  - PIN
- Bio-identification
  - Finger print
  - IRIS
  - Voice
  - DNA

LDAPs and Active Directory

- What is LDAP
  - Light Directory Access Protocol
  - What does that have to do with security?
- How LDAP is used
- Evolution of LDAP offerings
- Active Directory
  - A special case of LDAP
- Integrated multi-system identity management

Other Identify Management Infrastructure Components

- Kerberos
- Radius
- 4th Generation Firewalls
- Endpoint security

ACL – Access Control Language

- Applied at the Database and/or application level
- Level of abstraction
  - Data elements
  - Tools
- Issues
  - Unique to application
  - Varying degress of data access control
  - Integration with Role-based administration
  - Legacy impact and maintenance
  - Synchronization and expiration

Digital Certificate Authority

- PKI Infrastructure
- Verifying application IDs on the network
- NAMs and the enabled desktop
- The future of mobile
  - MDM
  - Evolving native security
  - The Certificate-based future

Application Security

- User specific function and data access controls
  - Data classification
  - Role-based
  - Tool access restrictions
- Advanced tools
  - Hardwired systems
  - Location specific functions
  - Risks(spoofing)

Advanced Identity Management

- Device detection and tracking
- Behavior tracking
- Profiling
- Real-time access controls

Quiz