Application Architecture

Security Review - Findings (1/3)

- LDAP Authentication and Connection
  - application currently connects to the LDAP directory as “anonymous”

  ➡implement proper authentication/authorisation mechanisms to restrict access

  ➡use an encrypted connection (SSL/TLS) and mutual authentication
- Data encryption
  - algorithm processes data in blocks of 16 bytes at a time, identical text blocks produce identical cipher-text blocks

  ➡verify suitability of the selected encryption algorithm (AES-128-ECB)

  ➡provide more information about encrypted and non-encrypted data fields

Application Architecture

Security Review - Findings (2/3)

- Access controls
  - feasibility of using ip filters, client certificates for Client PC access control
  - application architecture does not specify User authentication and authorisation details

  ➡provide authentication, authorisation policy details
- Database security

  ➡use an encrypted connection (SSL/TLS) and mutual authentication

  ➡missing information for data backups