ATC Android Security Essentials

1. **Permissions**
    a. Introduction
    b. Android Platform Architecture
    c. Android Security Architecture
        i. Application Signing
        ii. Installing Applications
    d. Permissions
        i. Why Permissions
        ii. Enforcing Permissions
    e. Levels of Protection
        i. Normal Permissions or Level-Zero Permissions
        ii. Dangerous Permissions or Level – One Permissions
        iii. Signature Permissions or Level- Two Permissions
        iv. Signature and System Permissions or Level – Three Permissions
    f. Application Level Permissions
        i. Adding System Permissions required by an application
        ii. Declaring permissions required by other applications
    g. Component Level Permissions
        i. Activity
        ii. Service
        iii. Content Providers
        iv. Broadcast Intents
    h. Extending Android Permissions
        i. Adding a new permission
        ii. Creating a permission group
        iii. Creating a permission tree
    i. LAB: Securing Application using permissions
        i. Creating an application to use permission
        ii. Creating permission and access it

2. **Managing the policy file**
    a. Introduction
    b. The manifest file
        i. Attributes of Manifest Tag
        ii. Attributes of Application Tag
    c. Modifying Application policy
        i. Application running with same Linux ID
        ii. Setting application permissions
        iii. Permissions for external applications

iv. External storage
v. Debugging mode
vi. Backup
d. LAB: Defining the application Policy File
i. Creating two application with the same Linux ID
ii. Backing up Data on cloud storage
iii. Debugging the Application
iv. Moving application of the internal memory of the device

3. User Data Privacy and Protection

a. Introduction
b. Data Security Principles
i. Confidentiality
ii. Integrity
iii. Availability
iv. The Mobile environment
v. Data States
c. Vulnerabilities and Attacks against Stored Data
i. Vulnerabilities of Stored Data
ii. Threats to Stored Data
d. Protection principles
e. Digital rights Management
i. Tips for Android coding vulnerabilities
f. LAB: Data Confidentiality and Protection
i. Ensuring Data Confidentiality
ii. Protecting Application Data with Permissions

4. Securing Storage

a. Introduction
b. Data Storage decisions
i. Privacy
ii. Data Storage Period
c. Storage Mechanisms
d. Shared Preferences
i. Creating a preference file
ii. Writing Preference
iii. Preference Activity
e. File
i. Creating a File
ii. Writing to a file
iii. Reading from a file

iv. File operation on an external storage

f. Cache

  i. Reading Preferences

g. Database

h. LAB: Data Storage Application

  i. Using Shared Preferences

  ii. File Storage Options

  iii. Storing data in cache

  iv. SQLite Database storage

  v. Retrieve GMAIL Account info using Account Manager