Pointing out Security Guidelines

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

“the code is more what you’d call guidelines than actual rules.”

Captain Barbosa’s

OWASP Top 10 Mobile Controls

OWASP Top 10 Mobile Controls

Classify data storage according to sensitivity

Store sensitive data on the server

Use a file encryption API

Restrict access to sensitive data

Do not store historical GPS/tracking on the device

1

Protect sensitive data on the mobile device

OWASP Top 10 Mobile Controls

Assume that shared storage is untrusted

Schedule data deletion

Consider the security of the whole data lifecycle

Only collect and disclose data required for business use

Use non-persistent identifiers

1

Protect sensitive data on the mobile device

OWASP Top 10 Mobile Controls

Utilize longer term authorization tokens

Leverage encryption and key-store mechanisms

Utilize secure element

Allow users to change passwords on the device

Credentials as backups should be in encrypted form

2

Handle password credentials securely

OWASP Top 10 Mobile Controls

Only use visual passwords with sufficient entropy

Allow repeated patterns to foil smudge-attacks

Confirm the entropy of all passwords

Ensure passwords and keys are not visible

Do not store passwords or secrets in the application binary

2

Handle password credentials securely

OWASP Top 10 Mobile Controls

Assume that the network layer is not secure

Enforce the use of an end-to-end secure channel

Use strong and well-known encryption algorithms

Use certificates signed by trusted CA providers

Disallow sensitive data to be send by SMS, MMS or notifications

3

Ensure sensitive data is protected during transit

OWASP Top 10 Mobile Controls

Require appropriate strength user authentication

Require authentication credentials to be passed with any subsequent request

Use unpredictable session identifiers with high entropy

Use additional authentication factors when possible

Use authentication that ties back to the end user's identity

4

Implement correct authentication, authorization, and session management

OWASP Top 10 Mobile Controls

Check code for any unintentional transfers

Periodically test backend services and OSs for vulnerabilities

Ensure the server is running with hardened configurations

Retain adequate logs on the backend to detect incidents

Employ rate limiting and throttling on a per-user/IP basis

5

Keep the backend APIs and platform secure

OWASP Top 10 Mobile Controls (Continued)

OWASP Top 10 Mobile Controls

Vet the authenticity of third-party codes

Track all third-party frameworks used in the application for security patches

Validate all data received from and sent to non-trusted third-party apps

6

Secure data integration with third party services

OWASP Top 10 Mobile Controls

Create a privacy policy covering the usage of personal data

Identify if your application is collecting PII

Conduct audits to check for unintended leaks

Keep a record of consent to the transfer of PII

Ensure collection mechanism doesn't overlap with any other

7

Collect and store consent for the use of user's data

OWASP Top 10 Mobile Controls

Maintain logs of access in a non-repudiable format

Check for anomalous usage patterns

Authenticate API calls

Warn user and obtain consent for cost implications

Implement best practices

8

Prevent unauthorized access to paid-for resources

OWASP Top 10 Mobile Controls

Design applications to allow updates for security patches

Distribute apps through official app-stores to provide a safety-net

Provide feedback channels for users to report security problems

9

Secure distribution of mobile applications

OWASP Top 10 Mobile Controls

Run interpreters at minimal privilege levels

Appropriately define comprehensive escape syntax

Utilize fuzz test interpreters

Utilize sandbox interpreters

10

Identify any runtime interpretation of code for errors

Mobile Control Guidelines

Mobile Control Guidelines

Avoid loading too many apps

Be cautious when uploading photos

Manage and control all devices

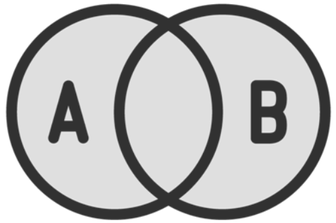
Conduct security assessments

Only allow trusted applications

Reconsider location-based features

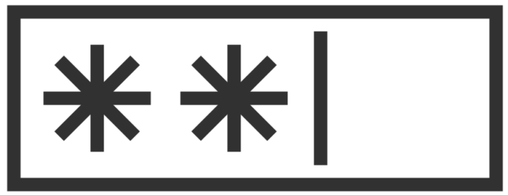
Mobile Control Guidelines

Disable Bluetooth when not in use



Avoid connecting to two networks

Do timely backups

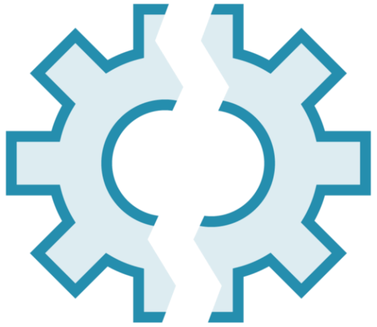


Use strong passwords

Set the idle timeout

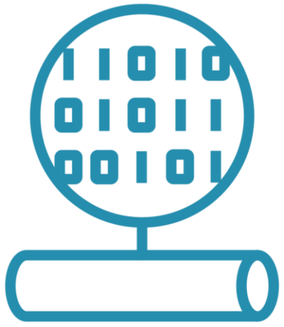
Use lockout and wipe features

Mobile Control Measures

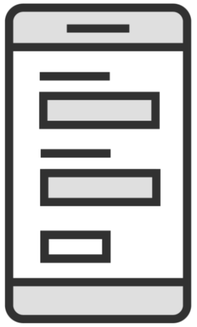


Disallow rooted or jailbroken devices

Keep the OS and all Apps updated



Encrypt hardware

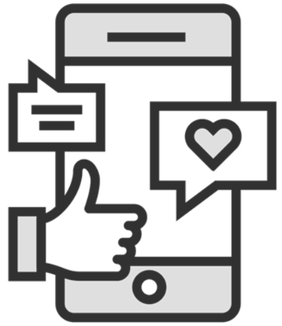


Harden up browsers

Review your MDM policies

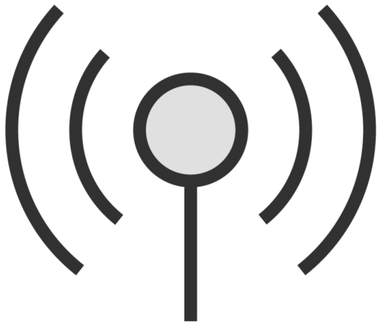
Filter email forwarding barriers

Mobile Control Measures



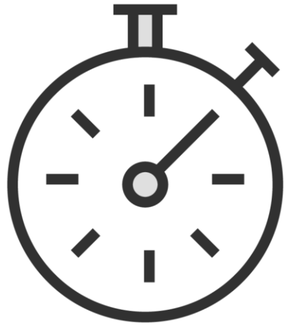
Use signed applications

Use auto lock



Require permission to join Wi-fi

Incorporate a data policy



Determine a timeout

Train users

Learning Check

Learning Check

- Never assume it's secure
- No sideloading
- Secure communications
- Timeout policy
- Train them

Up Next:
Hacking IoT and OT