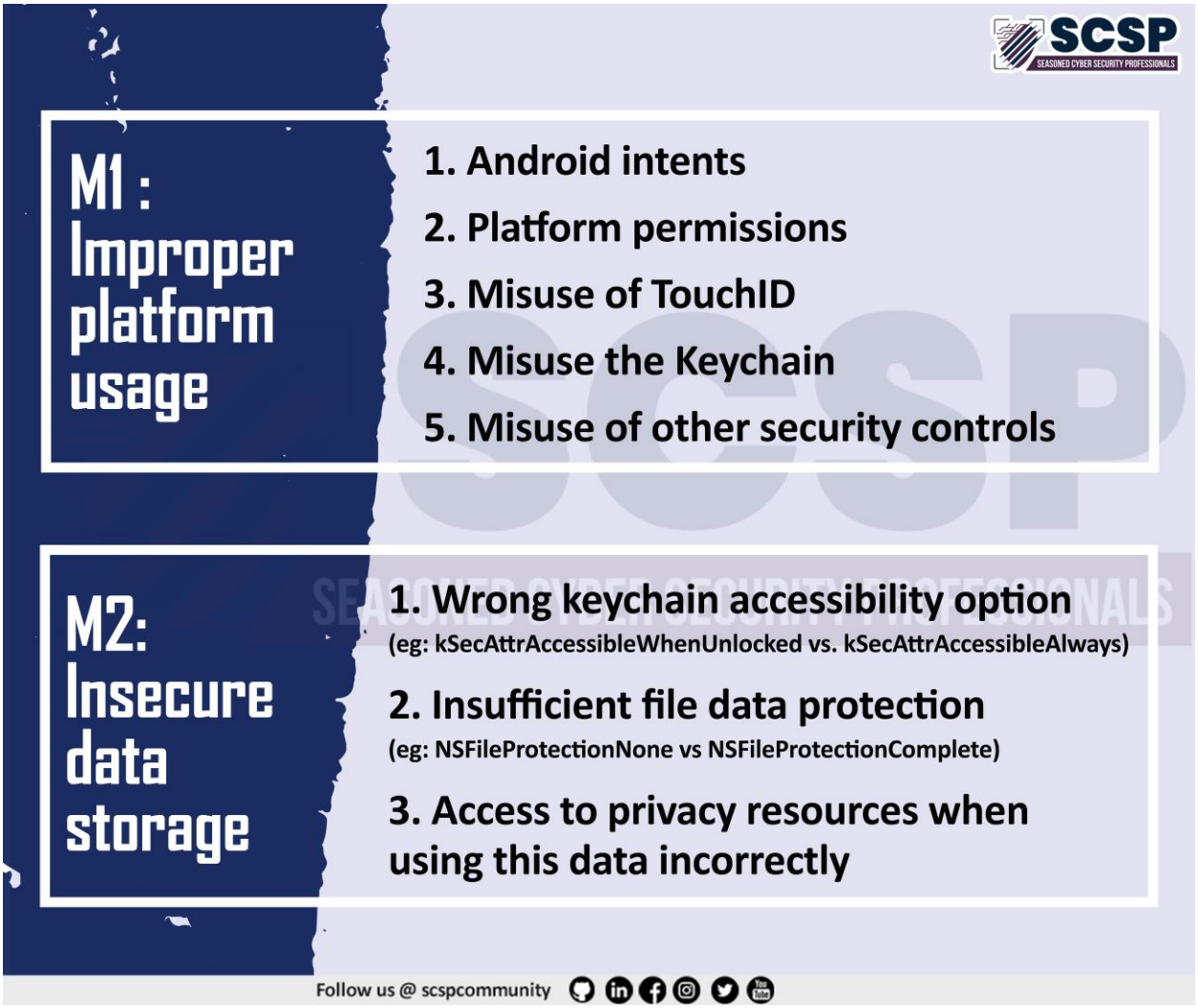
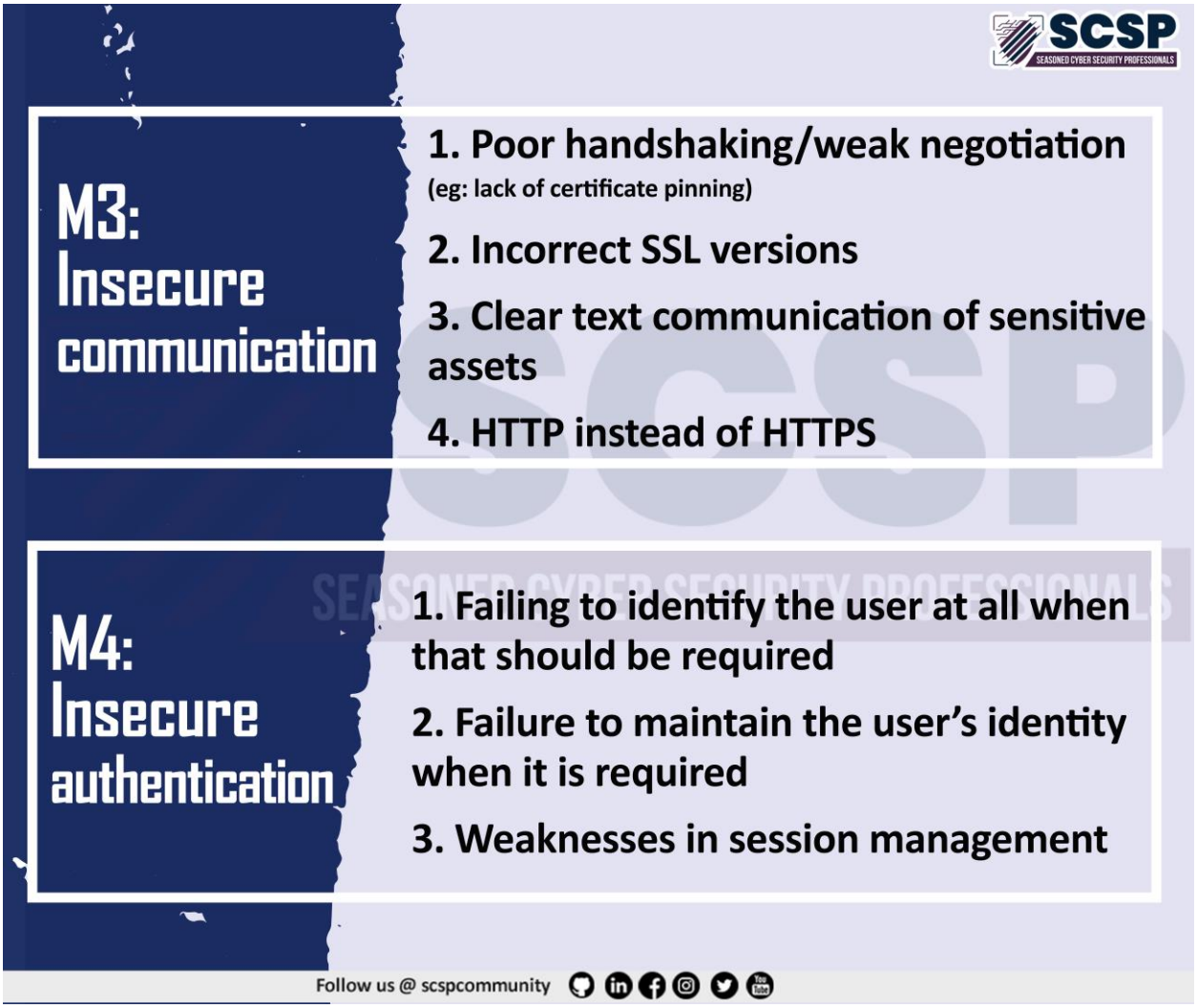
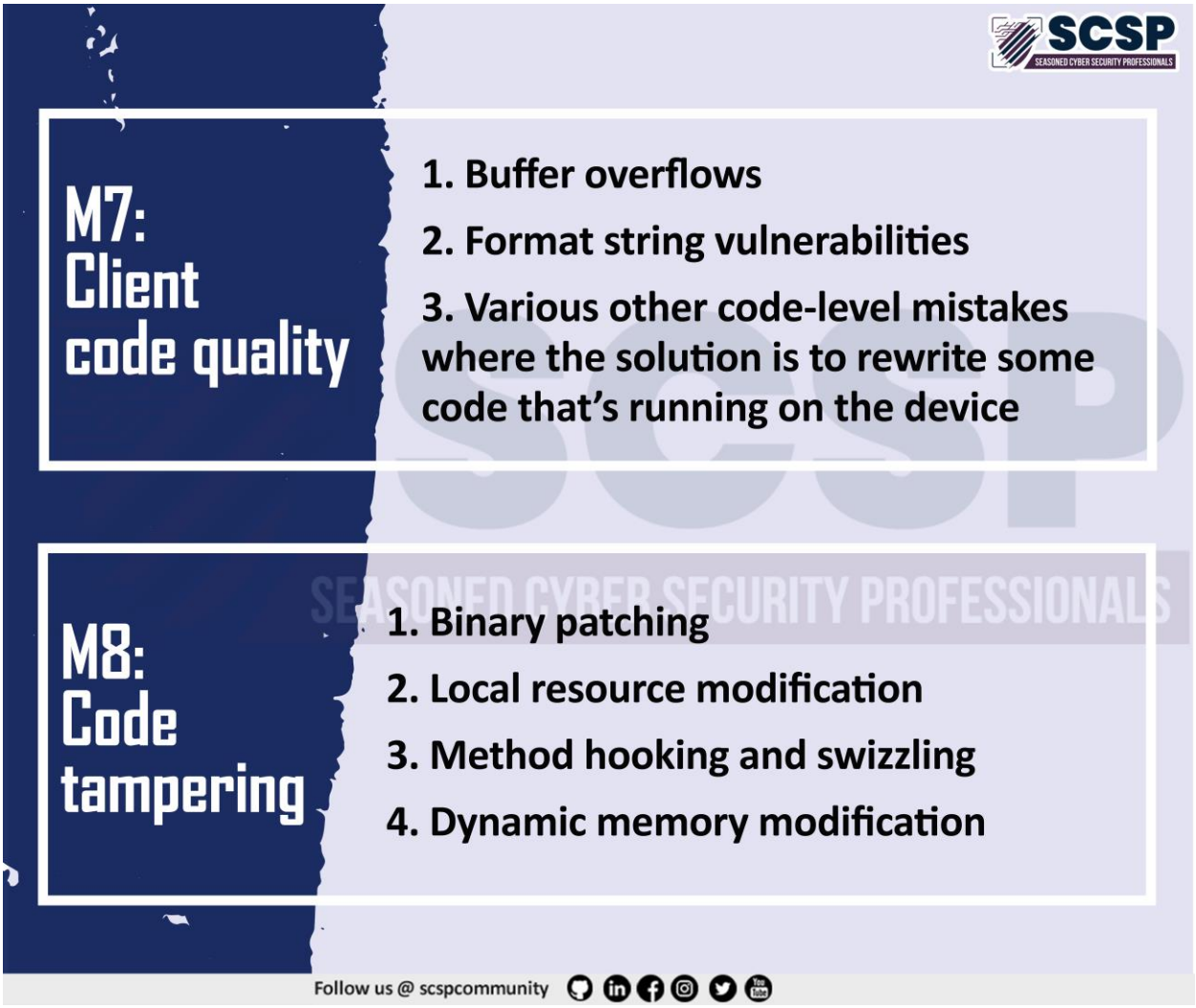
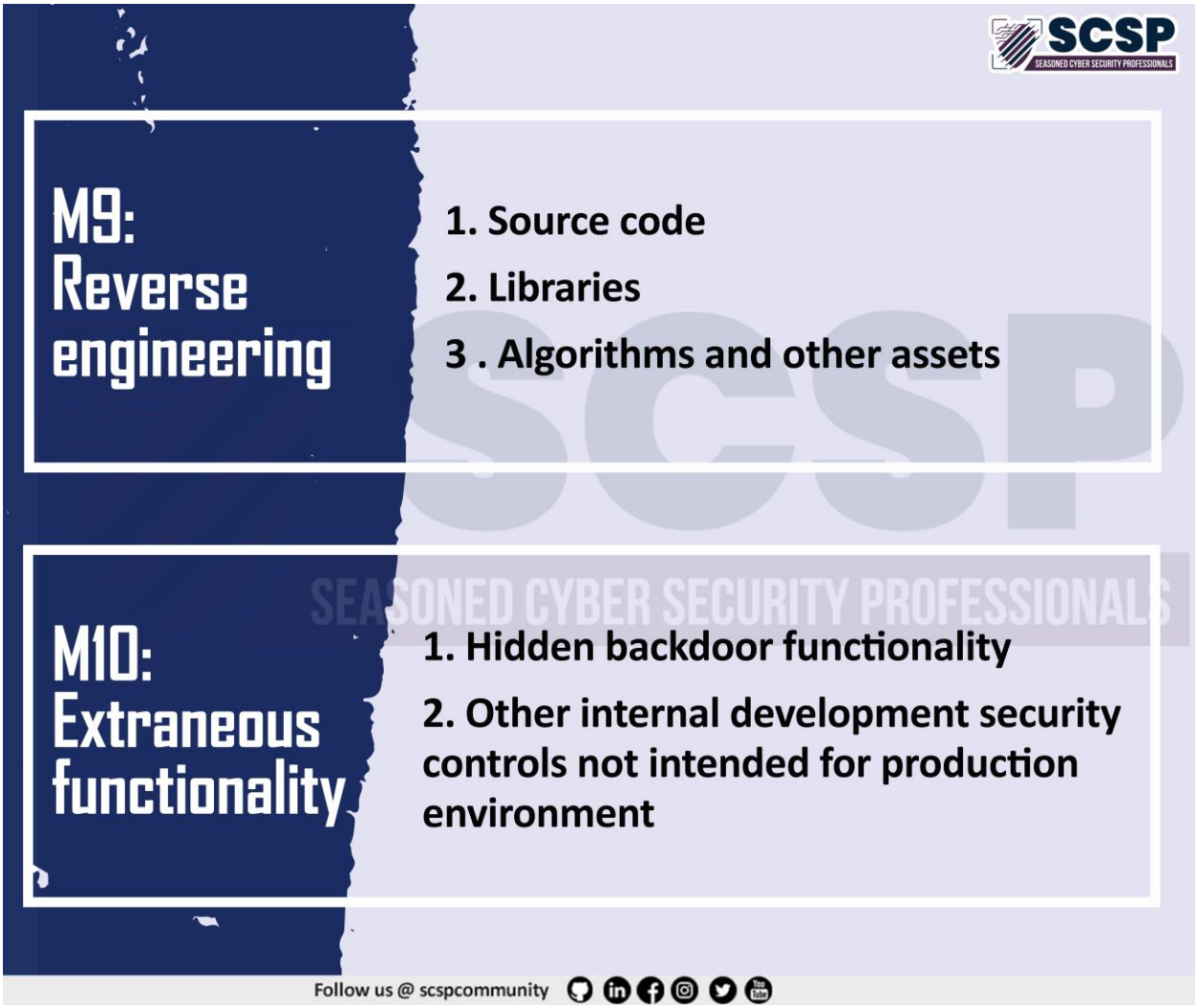

SCSP
SEASONED CYBER SECURITY PROFESSIONALS
OWASP
Mobile Top 10
Where to look for them?
Follow us @ scspcommunity


SCSP
SEASONED CYBER SECURITY PROFESSIONALS
M1 : Improper platform usage
1. Android intents
2. Platform permissions
3. Misuse of TouchID
4. Misuse the Keychain
5. Misuse of other security controls
M2: Insecure data storage
1. Wrong keychain accessibility option
(eg: kSecAttrAccessibleWhenUnlocked vs. kSecAttrAccessibleAlways)
2. Insufficient file data protection
(eg: NSFileProtectionNone vs NSFileProtectionComplete)
3. Access to privacy resources when using this data incorrectly
Follow us @ scspcommunity


SCSP
SEASONED CYBER SECURITY PROFESSIONALS
M3: Insecure communication
1. Poor handshaking/weak negotiation
(eg: lack of certificate pinning)
2. Incorrect SSL versions
3. Clear text communication of sensitive assets
4. HTTP instead of HTTPS
M4: Insecure authentication
1. Failing to identify the user at all when that should be required
2. Failure to maintain the user's identity when it is required
3. Weaknesses in session management
Follow us @ scspcommunity


SCSP
SEASONED CYBER SECURITY PROFESSIONALS
M5:
Insufficient cryptography
1. Poor Key Management Processes
2. Creation and Use of Custom Encryption Protocols
3. Use of Insecure and/or Deprecated Algorithms
M6:
Insecure authorization
1. Failures in authorization
(e.g., authorization decisions in the client side forced browsing, etc.)
2. Able to execute over-privileged functionality
Follow us @ scspcommunity


SCSP
SEASONED CYBER SECURITY PROFESSIONALS
M7:
Client
code quality
1. Buffer overflows
2. Format string vulnerabilities
3. Various other code-level mistakes where the solution is to rewrite some code that's running on the device
M8:
Code
tampering
1. Binary patching
2. Local resource modification
3. Method hooking and swizzling
4. Dynamic memory modification
Follow us @ scspcommunity


SCSP
SEASONED CYBER SECURITY PROFESSIONALS
M9: Reverse engineering
1. Source code
2. Libraries
3 . Algorithms and other assets
M10: Extraneous functionality
1. Hidden backdoor functionality
2. Other internal development security controls not intended for production environment
Follow us @ scspcommunity