CompTIA Mobile App Security+ Certification Exam (iOS Edition) Live exam IOS-001 Beta Exam IO1-001

INTRODUCTION
This exam will certify that the successful candidate has the knowledge and skills required to securely create a native iOS mobile application, while also ensuring secure network communications and backend Web services.

Test Purpose: The CompTIA Mobile App Security+ Certification Exam (iOS Edition) is suited for those individuals with at least 24 months of application development experience, as well as solid familiarity with the iOS SDK and principles of secure application development.

The successful candidate should have the knowledge and skills to:

- Describe fundamental principles of application security
- Describe the security model of iOS devices
- Describe common threats to mobile application security
- Develop moderately complex applications using the iOS SDK
- Describe Web services security model and vulnerabilities
- Properly implement SSL/TLS for Web communications
- Utilize the security features of the iOS operating system and APIs
- Properly implement secure coding techniques
- Avoid insecure retention of data in memory
- Describe common implementations of cryptography such as PKI
- Leverage encryption for storage and/or communications
- Harden an application against attack to levels appropriate for the risk model of the application

Prerequisite knowledge: Objective-C programming, iOS SDK, SQL coding, mobile and app security essentials, implementing encryption

Domain	% of Examination
1.0 Application Security and SDLC Fundamentals	11%
2.0 Objective-C Coding	14%
3.0 iOS SDK, APIs, and Security Features	21%
4.0 Web Service and Network Security	18%
5.0 Data Security and Implementing Encryption	23%
6.0 Application Hardening	13%
Total	**100%**

Copyright ©2013 by the Computing Technology Industry Association. All rights reserved.
The CompTIA Mobile App Security+ Certification Exam Objectives are subject to change without notice.

www.ITCareerFinder.com www.CompTIA.org

CompTIA Authorized Materials Use Policy

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites, aka 'brain dumps'. Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies webpage:
http://certification.comptia.org/Training/testingcenters/policies.aspx

Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to
abide by the CompTIA Candidate Agreement
(http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx) at the time of exam delivery.

If a candidate has a question as to whether study materials are considered unauthorized (aka brain dumps), he/she should perform a search using CertGuard's
engine, found here:
http://www.certguard.com/search.asp

Or verify against this list:
http://certification.comptia.org/Training/testingcenters/policies/unauthorized.aspx

**Note: The lists of examples provided in bulleted format below each objective are not exhaustive lists. Other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document.

CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

Copyright ©2013 by the Computing Technology Industry Association. All rights reserved.
The CompTIA Mobile App Security+ Certification Exam Objectives are subject to change without notice.

www.ITCareerFinder.com www.CompTIA.org

1.0 Application Security and SDLC Fundametals

1.1 Identify reasons for significance of secure mobile development.
- U.S. Regulatory requirements: PCI, HIPAA, FFIEC, FISMA
- International requirements: E.U. privacy
- Business requirements
- Consumer expectations (including privacy)

1.2 Describe security risks which are unique or higher for mobile technologies/devices.
- Lost/stolen device (physical access)
- Untrusted Wi-Fi networking (DNS attack, MITM)
- Users running modified OS (jailbroken)
- Telephony-related attacks (SMiShing, MitMo, toll fraud)

1.3 Compare the relative severity of security issues.
- Unprotected web interfaces
- Vulnerability to SQL Injection
- Storage of passwords, sensitive data without encryption
- Transmission without encryption (TLS/SSL)

1.4 Explain a secure development process throughout application development.
- Security testing/review on release (and during development)
- Business requirements
- Specifications
- Threat model/architectural risk analysis
- Code review
    - Automated
    - Manual
- Perform security testing
    - Fuzzing
    - Security functionality
    - Dynamic validation
    - Risk based testing
    - Penetration testing
- Types of documentation
    - Regulatory or corporate policy security or privacy requirements
- Schedule on-going security tests post-OS upgrades

1.5 Summarize general application security best practices.
- Sanitizing input, input validation
- Contextually appropriate output escaping
- Good design considerations:
    - Logic in applications

Copyright ©2013 by the Computing Technology Industry Association. All rights reserved.
The CompTIA Mobile App Security+ Certification Exam Objectives are subject to change without notice.

www.ITCareerFinder.com www.CompTIA.org

    - Storage of variables
    - Database design
- Debugging
- Error handling
- Secure storage
- Secure communications
- Authentication and authorization
- Session management
- Ensuring Application and data integrity
- Security by design vs. obscurity
- Sandbox

1.6 Identify the major architectural risks to weaknesses in an application.

- Build an architecture diagram of an application (including backend services), along with descriptions of each component
- Establish a deep and comprehensive understanding of the application and its components
- Break the architecture into specific security zones for individual consideration
- For each zone, articulate and enumerate each of the following:
    - Who has access to the zone?
    - What would motivate someone to attack the system?
    - What would an attacker target, specifically, in each zone? (e.g., data, functions)
    - How could each target be attacked? (Reference Microsoft's STRIDE process.)
    - What would be the impact to the business of a successful attack?
    - What remediation could be implemented to reduce the likelihood of successful attack?
- Recommend and justify remediation based on their corresponding likelihood and magnitude of impact vs. their costs to the business

2.0 Objective-C Coding

2.1 Explain the Objective-C language and design.

- Instance variables
- Methods
- Method Cache
- Integrating C into Objective-C

2.2 Demonstrate proper handling of sensitive data in memory.

- Level 3, use code example selection
- Cleaning up sensitive values used temporarily (passcodes, keys, credit card info)

Copyright ©2013 by the Computing Technology Industry Association. All rights reserved.
The CompTIA Mobile App Security+ Certification Exam Objectives are subject to change without notice.

www.ITCareerFinder.com www.CompTIA.org

- Show ability to select correct code, which does not store and which clears values

2.3 Explain Objective-C framework paradigms and related security impacts.
- Nuances to class construction, pose and replace functions (methods, classes, etc), and other design nuances which can be exploited
- Objective-C interfaces into C Land (dlsym, dladdr, Objective-C library calls for replacing methods, etc)

2.4 Demonstrate proper interaction with iOS security facilities and objects.
- Code examples of various implementations (correct and incorrect), and distinguish between incorrect and correct usage
- Security frameworks (dataprotection), keychain access, read/write access to files within an application, memory handling, ARC (Automatic Reference Counting), SQLite DB querying (Level 4)

3.0 iOS SDK, APIs, and Security Features

3.1 Summarize the security features of the platform.
- Code signing
- Sandbox
- Data at rest encryption
- Generic native exploit mitigation features
    - ASLR
    - Non executable memory
    - Stack smashing protection

3.2 Explain the data protection API.
- Automatically setup when passcode is set
- Various levels of protection, driven by developer
    - Complete protection
    - Protected unless open
    - Protected until first user authentication
    - No protections

3.3 Explain the features of the security framework.
- Common Crypto Libraries
    - Symmetric encryption
    - HMAC
    - Digests
- Generating secure random numbers

Copyright ©2013 by the Computing Technology Industry Association. All rights reserved.
The CompTIA Mobile App Security+ Certification Exam Objectives are subject to change without notice.

www.ITCareerFinder.com www.CompTIA.org

3.4 Explain the security and limitations of the keychain.

- Keychain access groups
- Managing certificates and keys
- What does not belong in the keychain
- How keychain can be accessed or compromised (e.g., physical access, backups)

3.5 Demonstrate proper use of keychain for storing sensitive data.

- Select correct code, using enumeration

4.0 Web Service and Network Security

4.1 Summarize the risks in performing Web and network communications.

- Clear text transmission of data
- Man-in-the-middle attacks
- Cellular proxy attack (provisioning profile)
- Insufficient validation of certificates / certificate chain
- SSL compromise
- DNS hijacking

4.2 Implement an SSL session with validation.

- Validate originated from a trusted CA
- Validate the certificate has not been revoked
- Describe how to implement / validate client-side certificates
- SSL pinning
- If using CFNetwork ensure validation on expiry, root, and chain is enabled
- Use secure transport API to manage cipher suites
- Set SSL protocol type and versions

4.3 Explain common threats to Web services.

- Information disclosure
- Brute forcing
- Fuzzing
- SQL injection
- Directory traversal

4.4 Distinguish sound security protections for authentication.

- Brute forcing PIN locally

Copyright ©2013 by the Computing Technology Industry Association. All rights reserved.
The CompTIA Mobile App Security+ Certification Exam Objectives are subject to change without notice.

www.ITCareerFinder.com www.CompTIA.org

- Brute forcing authentication against Web service
- Not using basic authentication
- Not passing server/service credentials from application

4.5 Describe proper implementation of session security.
- Highly random token
- Expire on timeout or exit
- Store in memory not in data
- Avoid static user token
- UDID deprecation

5.0 Data Security and Implementing Encryption

5.1 Explain a secure data storage and encryption implementation.
- Key storage and retention
- Key derivation - Why 10,000 rounds of PBKDF2 is better than 3,000
- Master keys
- Key strength
- Cipher Specifications
- Forensic trace
- Storage of data in protected APIs
- Built-in encryption vs. custom encryption
- File permissions and using strong passwords for database security
- How to hash sensitive data and seed of passwords
- Storing more data externally on servers
- Not storing data outside of the applications security
- Do not store sensitive data, if you can avoid it
- Protecting data at rest while the device is locked

5.2 Demonstrate knowledge of proper implementation of encryption in iOS.
- Common cryptor
- Good design considerations:
    - Logic in applications
- Certificate and key exchange
- Authentication and authorization
- Session management
- Decryption as authentication, not after

5.3 Describe Apple Data Encryption APIs.
- PIN vs. complex passphrase
- Data protection APIs
- Keychain and vulnerabilities

Copyright ©2013 by the Computing Technology Industry Association. All rights reserved.
The CompTIA Mobile App Security+ Certification Exam Objectives are subject to change without notice.

www.ITCareerFinder.com www.CompTIA.org

- Demonstrate knowledge of Apple's encrypted file system
- Journal

5.4 Demonstrate understanding of best practices for secure data deletion.
- Wiping memory
- Wiping SQLite records
- DOD 5220.22-M data destruction standard

5.5 Explain nature and extent of data recovery techniques for iOS.
- Binary imaging and carving, could keys/passwords be recovered by a raw dump?
- How jailbreaking can lead to access to data protected by permissions.
- SQLite database, when does data get deleted, does is hang around?
- Recovery data from backup, iCloud security
- Flash NAND storage, if something is deleted is it actually deleted?
- Custom RAM disks, booting another kernel to gain access to the file system
- Live Forensics, what is being stored in memory, can this be dumped?

5.6 Explain types and sensitivity of particular data, and how it can leak.
- Usage logs, session logs, debugging data
- Phone book, calendar, notes
- Content of private communications messages, IM, etc.
- Account and log in information
- Transaction and payment data
- Web caches, cookies and other 'temporary' data
- Location data, Cell tower and GPS information
- Wi-Fi and Bluetooth passwords, IP address and routing information
- Audio recording and video
- Picture meta data

6.0 Application Hardening

6.1 Explain application object binaries and tools.
- Apple Digital Rights Management
- Mach-O object format
- Symbol table definitions
- Class-dump
- Dumping memory
- Binary stripping

6.2 Explain Objective-C debugging.
- Attaching to processes

Copyright ©2013 by the Computing Technology Industry Association. All rights reserved.
The CompTIA Mobile App Security+ Certification Exam Objectives are subject to change without notice.

www.ITCareerFinder.com www.CompTIA.org

- Common debugger commands
- Code obfuscations
- Dynamic code injection
- Debugging detection techniques

6.3 Describe forms of abusive runtime manipulation.

- Attaching to processes using cycript
- Bypassing application UI locks
- Overriding application methods
- Manipulating instance variables
- Foundation class attacks

6.4 Summarize counter-runtime abuse techniques.

- Jailbreak detection
- Runtime class validation
- Process trace checks
- Tamper response
- Counter-debugging techniques
- Code obfuscations
    - Optimizations
    - Inline functions
    - Encrypted payloads

Copyright ©2013 by the Computing Technology Industry Association. All rights reserved.
The CompTIA Mobile App Security+ Certification Exam Objectives are subject to change without notice.

www.ITCareerFinder.com www.CompTIA.org