Security data management for app devs

@vixentael for  try! Swift

COSSACK LABS

Anastasiia Voitova

Head of customer solutions, security software engineer @CossackLabs

Master of designing e2ee protocols for not-chatting apps.

Ex full time iOS apps dev (iOS3..10).

Maintainer of OSS crypto lib Themis.

More a builder than a breaker.

@vixentael cossacklabs.com

training.cossacklabs.com

What we do today:

1. Talk about SSDLC, data, risks, threats, security controls.
2. Overview regulations and guidelines.
3. Take exercises on selecting security controls.
4. Discuss security tools and approaches.
5. Q&A

What we do today:

1. Talk about SSDLC, data, risks, threats, security controls.
2. Overview regulations and guidelines.
3. Take exercises on selecting security controls.
4. Discuss security tools and approaches.
5. Q&A

} *slides*

} *workbook*

Why apps need security?

1. Regulations (data protection, privacy, financial, medical, etc).

2. B2B:

3. B2C:

Why apps need security?

1. Regulations (data protection, privacy, financial, medical, etc).

2. B2B: business requirements (finance, legal, compliance, vendor-specific rules).

3. B2C:

Why apps need security?

1. Regulations (data protection, privacy, financial, medical, etc).

2. B2B: business requirements (finance, legal, compliance, vendor-specific rules).

3. B2C: users pressure (user care about their data).

security measures are very different for every app

Q&A

1. How to make security decisions, balancing between “no protection” and “paranoid defenses”.

2. How to avoid spending time on low priority security features and focus on “must have”.

Q&A

1. How to make security decisions, balancing between “no protection” and “paranoid defenses”.

define which security risks app is facing

2. How to avoid spending time on low priority security features and focus on “must have”.

triage security features based on risks they will protect from

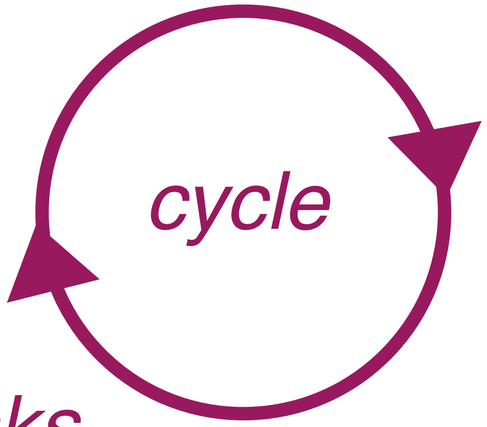
Q&A

1. How to make security decisions, balancing between “no protection” and “paranoid defenses”.

define which security risks app is facing

2. How to avoid spending time on low priority security features and focus on “must have”.

triage security features based on risks they will protect from



Secure software development lifecycle methodology (SSDLC)

MS SDL

www.microsoft.com/en-us/sdl

OWASP S-SDLC

www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project

3. OWASP SSDLC — a process that means * 2 points

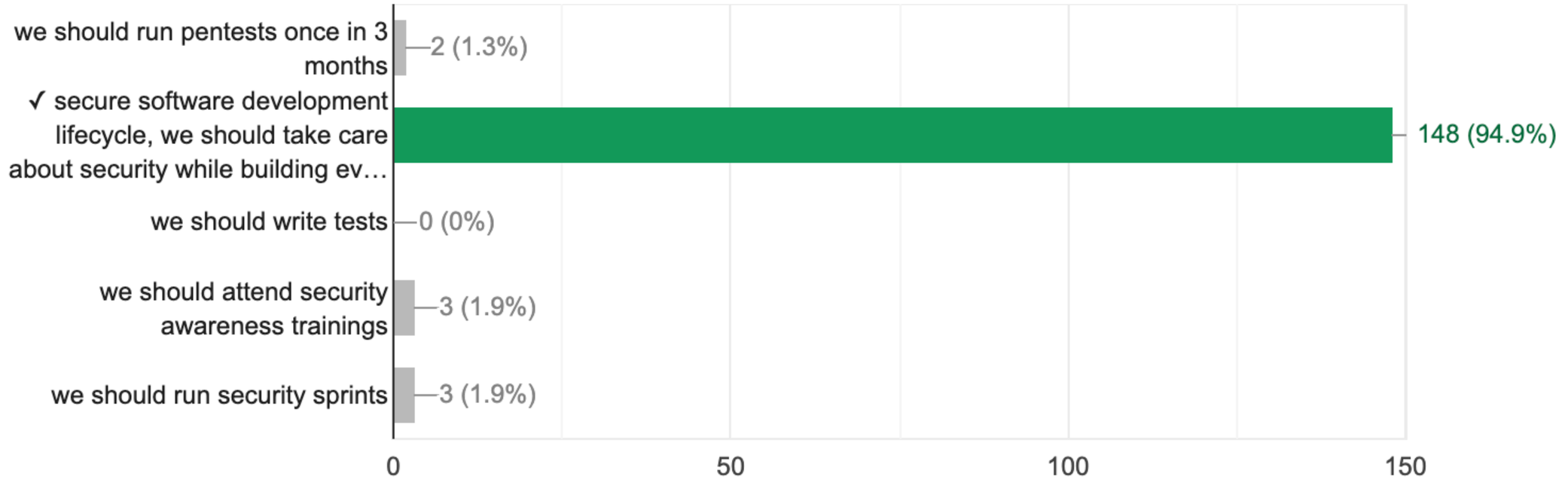
- ○ we should run pentests once in 3 months
- ○ secure software development lifecycle, we should take care about security while building every feature of our app
- ○ we should write tests
- ○ we should attend security awareness trainings

3. OWASP SSDLC — a process that means * 2 points

- we should run pentests once in 3 months
- secu… build…
- we sh…
- we sh…

3. OWASP SSDLC — a process that means

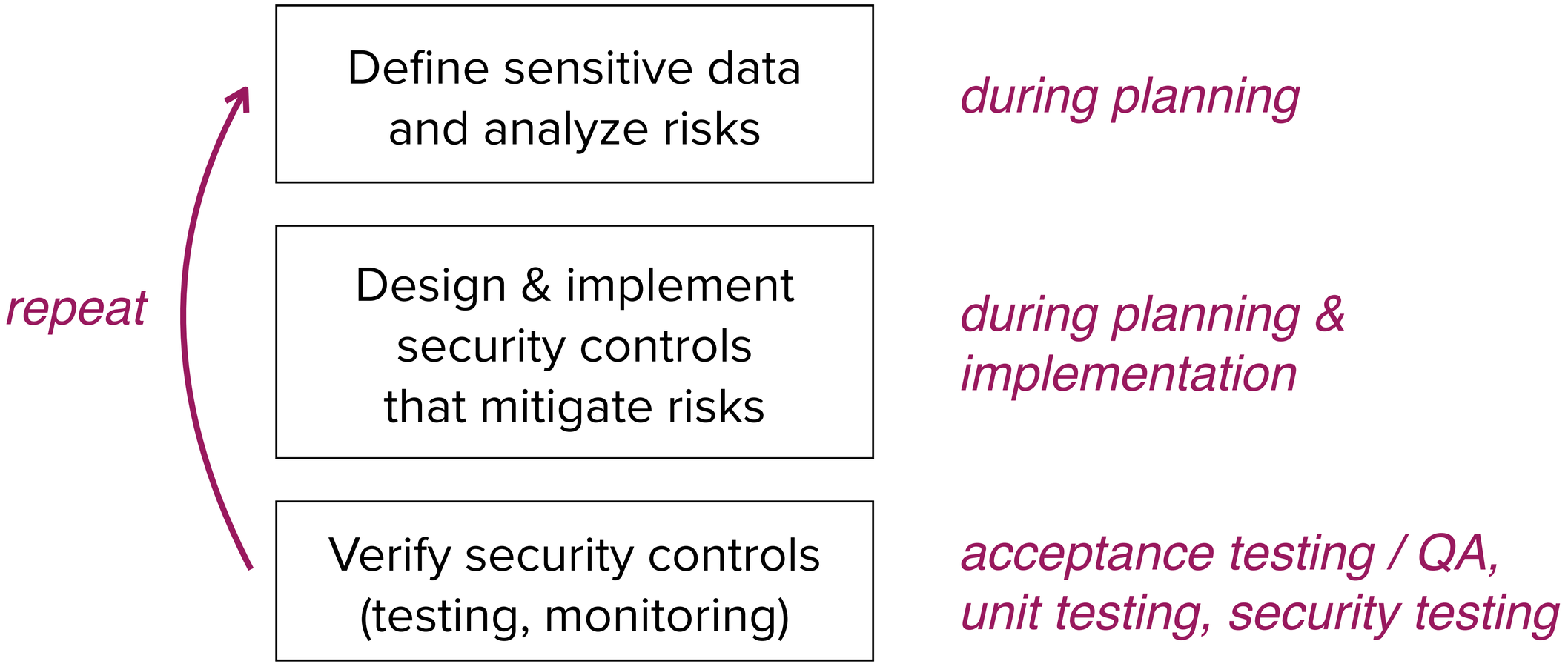
148 / 156 correct responses



SSDLC


Risk evaluation
Risk assessment
Threat model
Security plan
Secure coding
Security verification
Secure operations
Response

SSDLC in simple words



Sensitive data

– any kind of data, that will break business objectives or prosperity of those who use data, if leaked.

emails

backups

PII

videos from camera

logs

credentials

health data

chat history

financial data

geo-locations

cars remote control

screenshots

kids locations

Defining sensitive data

sensitive business data (PII, user credentials, fin data..)

tech data (keys, logs, accesses, IPs, backups..)

regulated data (user privacy, fin, medical..)

the more $$$ business will lose after losing data, the more sensitive it is

Regulations

available in workbook

General data security compliance: ISO/IEC 27002:2013, CCPA, NIST 800-171, FIPS 140-2, GDPR, DPA, Brazilian General Data Protection Act …

Finance: PCI DSS, PCI HSM, SWIFT Customer Security Controls, PSD2, FINMA, GLBA …

Healthcare: HIPAA, HITECH, ISO 27799:2016 …

Education: FERPA, GDPR ..

cheatsheet

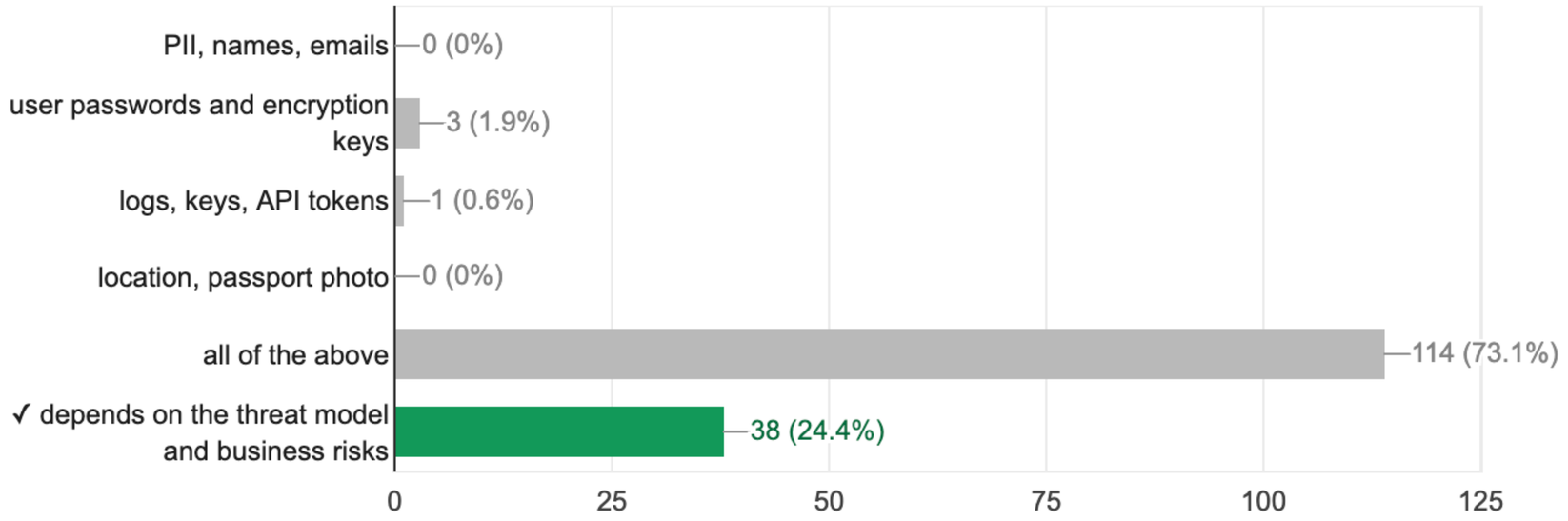
cossacklabs.com/blog/what-we-need-to-encrypt-cheatsheet.html

1. What is sensitive data that we need protect in the app: *

- ○ PII, names, emails
- ○ user passwords and encryption keys
- ○ logs, keys, API tokens
- ○ location, passport photo
- ○ all of the above
- ○ depends on the threat model and business risks

1. What is sensitive data that we need protect in the app:

38 / 156 correct responses



1. What is sensitive data that we r

- PII, names, emails
- user passwords and encryption k
- logs, keys, API tokens
- location, passport photo
- all of the above
- depends on the threat model and business risks

Risks

Business risk is the possibility a company will have lower than anticipated profits or experience a loss rather than taking a profit.

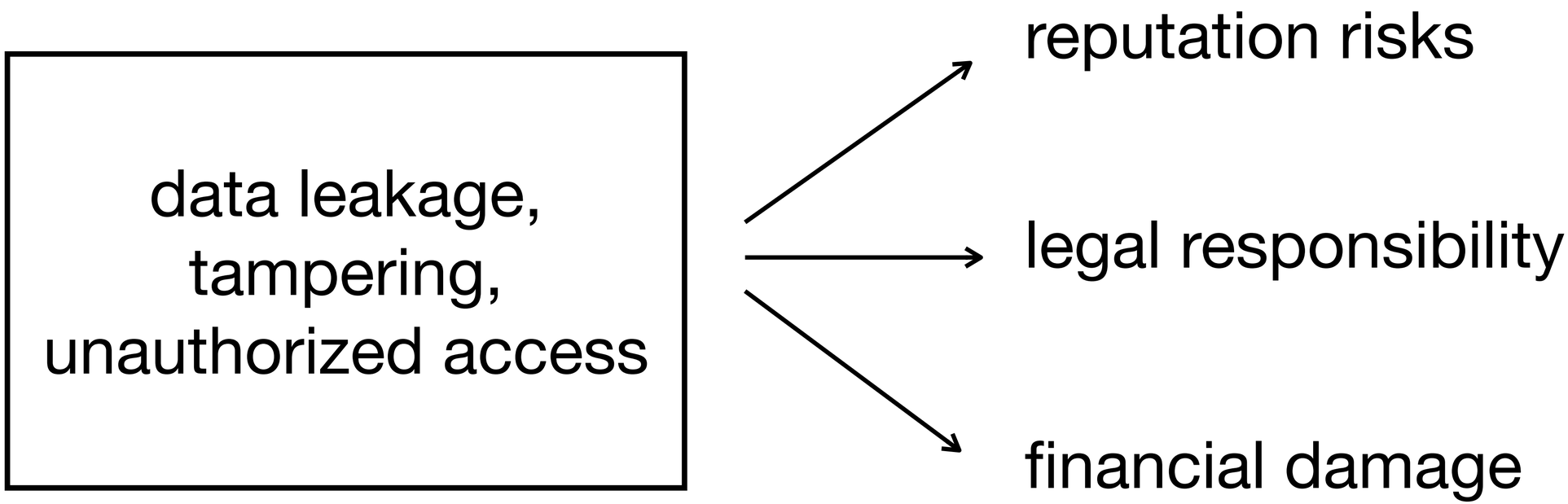
Risks

- unauthorized access
- disclosure
- disruption
- modification
- inspection
- recording
- destruction

- Strategic risks
- Operational risks
- Reputational risks
- Compliance risks

and many more

Risks to data



available in workbook

Risks to data

Data \ Risks	Access	Disclosure	Modification	Access denial
PII	High	High	High	Medium
Database	High	Critical	High	Critical
some data				

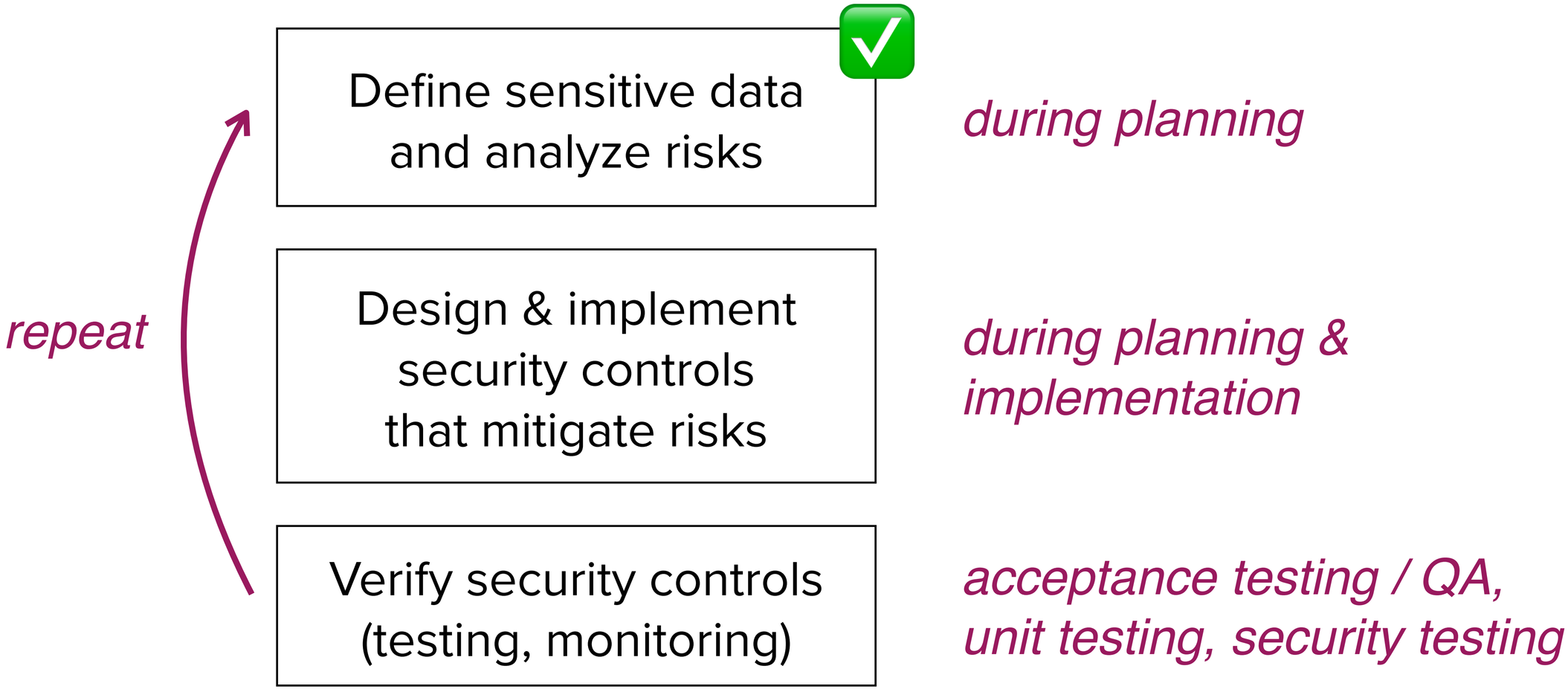
easy way to see the whole picture is to identify risks to data

OWASP Top10 mobile risks

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

owasp.org/www-project-mobile-top-10/

SSDLC in simple words



Q&A: security controls

available in workbook

Security controls proactive and reactive

Data security

Application security

Infrastructure security

Monitoring

Intrusion detection

Vulnerability management

Proactive controls

Data security	encryption
Access security	authentication, firewalls, OS
Node security	firewalls, compartmentalization, isolation, OS

Reactive controls

Data security	key management, integrity checks, authenticated crypto
Access security	credential management, access logging, jailbans
Node security	code security, monitoring, SIEM

Q&A: security controls

available in workbook

available in workbook

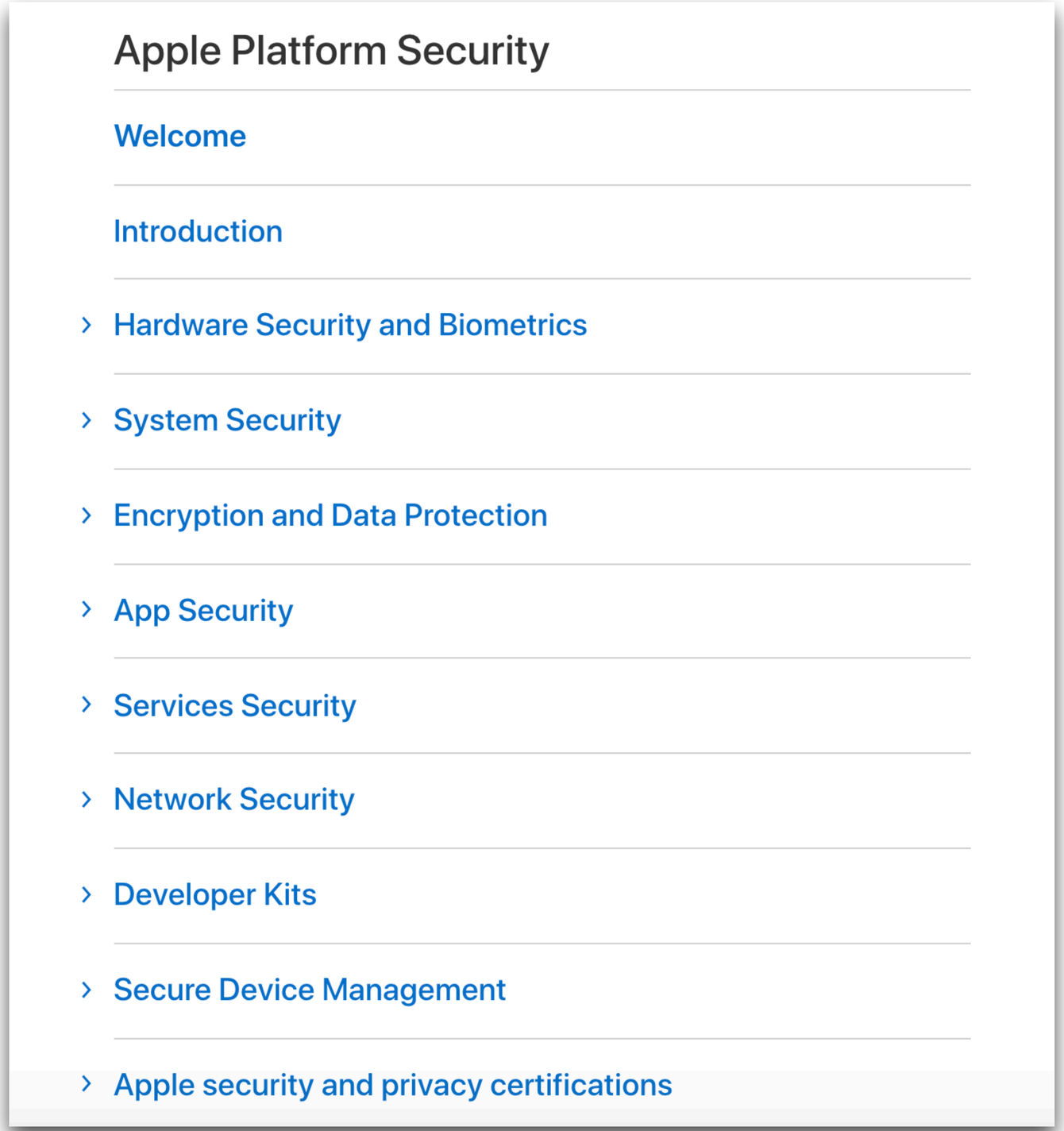
Security controls for iOS apps — check workbook

available in workbook

—Where to get these controls?

—Mobile application security design (standards and guidelines)

Apple Platform Security



support.apple.com/guide/security

App Store review guidelines

5.1 Privacy

Protecting user privacy is paramount in the Apple ecosystem, and you should use care when handling personal data to ensure you've complied with privacy best practices, applicable laws and the terms of the Apple Developer Program License Agreement, not to mention customer expectations. More particularly:

5.1.1 Data Collection and Storage

(i) Privacy Policies: All apps must include a link to their privacy policy in the App Store Connect metadata field and within the app in an easily accessible manner. The privacy policy must clearly and explicitly:

- Identify what data, if any, the app/service collects, how it collects that data, and all uses of that data.
- Confirm that any third party with whom an app shares user data (in compliance with these Guidelines) — such as analytics tools, advertising networks and third-party SDKs, as well as any parent, subsidiary or other related entities that will have access to user data — will provide the same or equal protection of user data as stated in the app's privacy policy and required by these Guidelines.
- Explain its data retention/deletion policies and describe how a user can revoke consent and/or request deletion of the user's data.

(ii) Permission Apps that collect user or usage data must secure user consent for the collection, even if such data is considered to be anonymous at the time of or immediately following collection. Paid functionality must not be dependent on or require a user to grant access to this data. Apps must also provide the customer with an easily accessible and understandable way to withdraw consent. Ensure your purpose strings

developer.apple.com/app-store/review/guidelines/#privacy

NIST SP 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations”

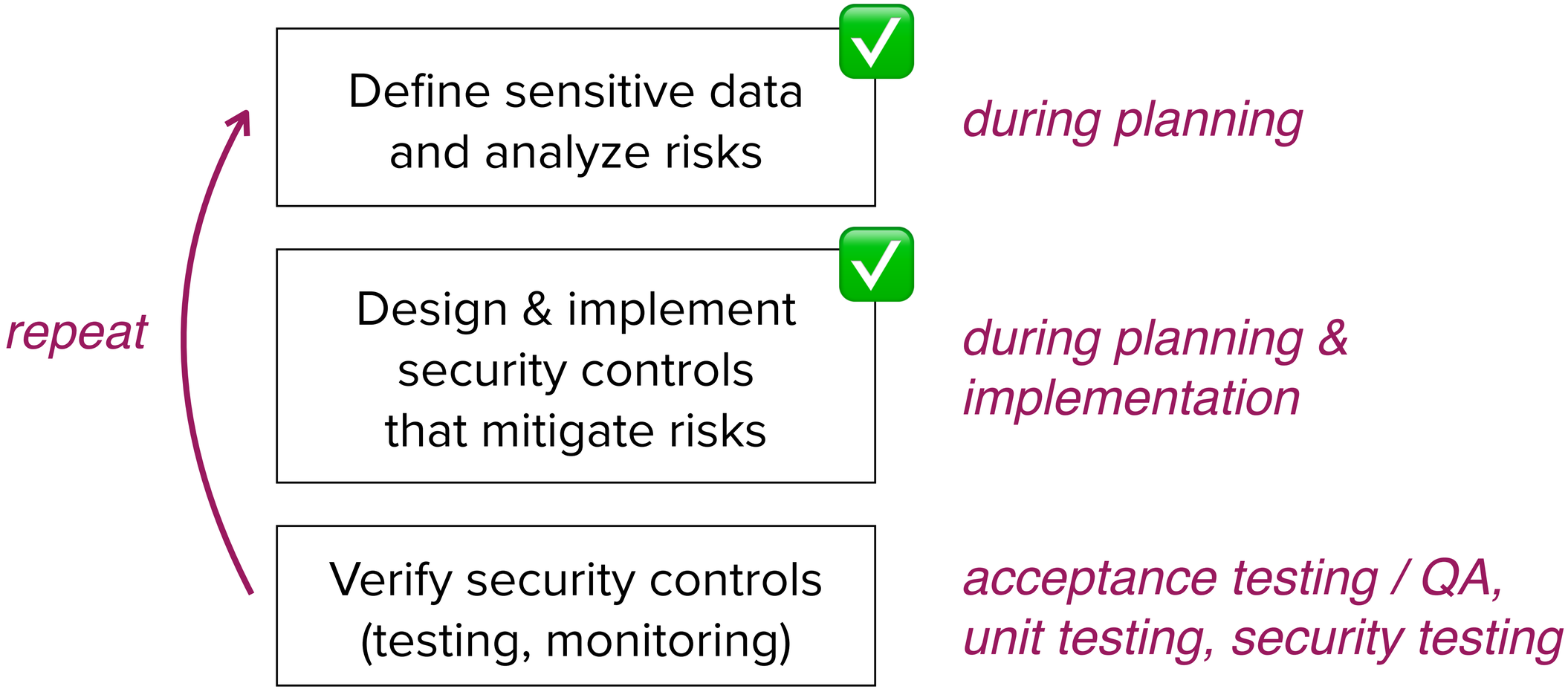
TABLE D-2: SECURITY CONTROL BASELINES[92]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12

462p PDF,
6 pages-long table of security controls themselves

csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

SSDLC in simple words



available in workbook

—How to make sure controls are working?

—Mobile application security verification and testing

Table 5 - iOS Vulnerability Descriptions, A Level.

Type	Description	Negative Consequence
Incorrect Permissions	Permissions allow accessing controlled functionality such as the camera or GPS and are requested in the program. Permissions can be implicitly granted to an app without the user's consent.	An app with too many permissions may perform unintended functions outside the scope of the app's intended functionality. Additionally, the permissions are vulnerable to hijacking by another app. If too few permissions are granted, the app will not be able to perform the functions required.
Exposed Communication-Internal and External	Internal communications protocols allow apps to process information and communicate with other apps. External communications allow information to leave the device.	Exposed internal communications allow apps to gather unintended information and inject new information. Exposed external communication (data network, Wi-Fi, Bluetooth, *etc.*) leave information open to disclosure or man-in-the-middle attacks.
Potentially Dangerous Functionality	Controlled functionality that accesses system-critical resources or the user's personal information. This functionality can be invoked through API calls or hard coded into an app.	Unintended functions could be performed outside the scope of the app's functionality.
App Collusion	Two or more apps passing information to each other in order to increase the capabilities of one or both apps beyond their declared scope.	Collusion can allow apps to obtain data that was unintended such as a gaming app obtaining access to the user's contact list.

NIST SP 800-163
"Vetting the security of mobile applications"

csrc.nist.gov/publications/detail/sp/800-163/rev-1/final

OWASP Mobile Application Security Verification Standard (MASVS)

https://github.com/OWASP/owasp-masvs

OWASP Mobile Security Testing Guide (MSTG)

https://github.com/OWASP/owasp-mstg

what to check

OWASP Mobile Application Security Verification Standard (MASVS)

https://github.com/OWASP/owasp-masvs

how to check

OWASP Mobile Security Testing Guide (MSTG)

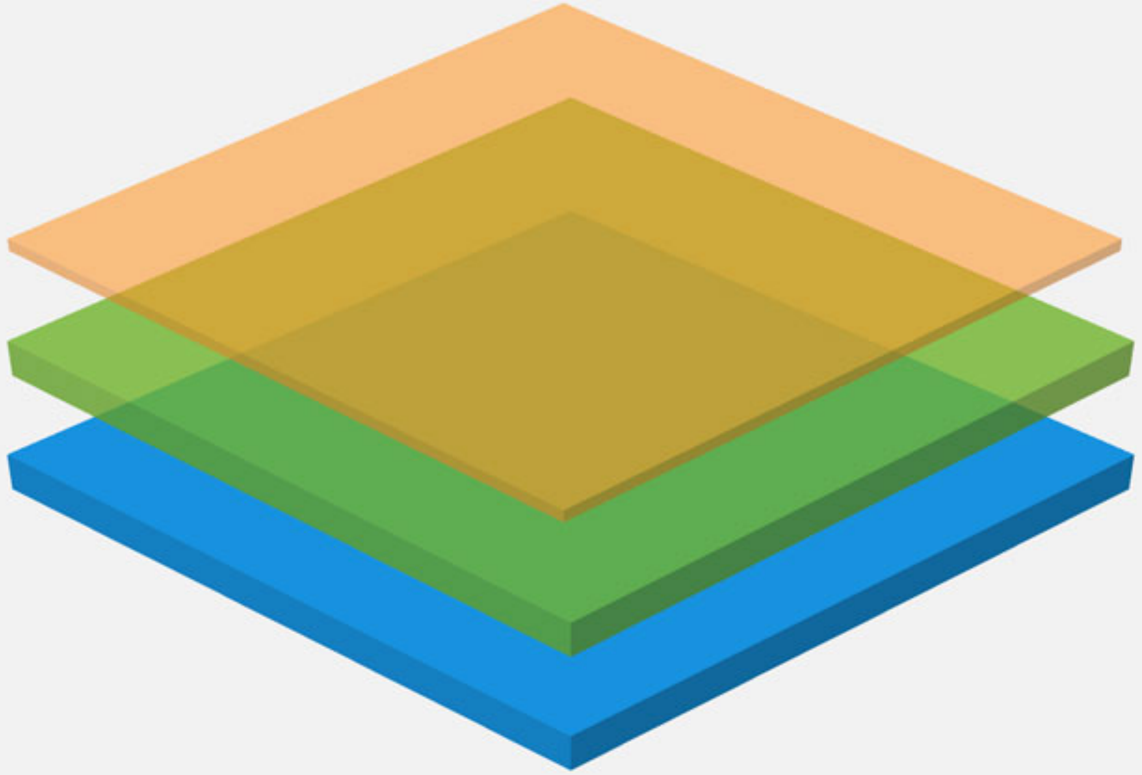
https://github.com/OWASP/owasp-mstg

MASVS

Mobile Application Security Requirements - iOS

ID	Detailed Verification Requirement	Level 1	Level 2	Status	Testing Pro
V1	**Architecture, design and threat modelling**				
1.1	All app components are identified and known to be needed.	✓	✓		-
1.2	Security controls are never enforced only on the client side, but on the respective remote endpoints.	✓	✓		-
1.3	A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.	✓	✓		-
1.4	Data considered sensitive in the context of the mobile app is clearly identified.	✓	✓		-
1.5	All app components are defined in terms of the business functions and/or security functions they provide.		✓	N/A	-
1.6	A threat model for the mobile app and the associated remote services has been produced that identifies potential threats and countermeasures.		✓	N/A	-
1.7	All security controls have a centralized implementation.		✓	N/A	-
1.8	There is an explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow a key management standard such as NIST SP 800-57.		✓	N/A	-
1.9	A mechanism for enforcing updates of the mobile app exists.		✓	N/A	-
1.10	Security is addressed within all parts of the software development lifecycle.		✓	N/A	-
V2	**Data Storage and Privacy**				
2.1	System credential storage facilities are used appropriately to store sensitive data, such as PII, user credentials or cryptographic keys.	✓	✓		Testing For Sensitive Data in Local Data Storage
2.2	No sensitive data should be stored outside of the app container or system credential storage facilities.				Testing For Sensitive Data in Local Data Storage
2.3	No sensitive data is written to application logs.	✓	✓		Testing For Sensitive Data in Logs
2.4	No sensitive data is shared with third parties unless it is a necessary part of the architecture.	✓	✓		Testing Whether Sensitive Data Is Sent To Third Parties
2.5	The keyboard cache is disabled on text inputs that process sensitive data.	✓	✓		Testing Whether the Keyboard Cache Is Disabled for Text Input Fields
2.6	No sensitive data is exposed via IPC mechanisms.	✓	✓		Testing Whether Sensitive Data Is Exposed via IPC Mechanisms
	No sensitive data, such as passwords or pins, is exposed through the user interface.	✓	✓		Testing for Sensitive Data Disclosure Through the User Interface

MASVS L1/L2



R – Resiliency Against Reverse Engineering and Tampering

L2 – Defense-in-Depth

L1 – Standard Security

MASVS: Network

Security Verification Requirements

#	MSTG-ID	Description	L1	L2
5.1	MSTG-NETWORK-1	Data is encrypted on the network using TLS. The secure channel is used consistently throughout the app.	✓	✓
5.2	MSTG-NETWORK-2	The TLS settings are in line with current best practices, or as close as possible if the mobile operating system does not support the recommended standards.	✓	✓
5.3	MSTG-NETWORK-3	The app verifies the X.509 certificate of the remote endpoint when the secure channel is established. Only certificates signed by a trusted CA are accepted.	✓	✓
5.4	MSTG-NETWORK-4	The app either uses its own certificate store, or pins the endpoint certificate or public key, and subsequently does not establish connections with endpoints that offer a different certificate or key, even if signed by a trusted CA.		✓
5.5	MSTG-NETWORK-5	The app doesn't rely on a single insecure communication channel (email or SMS) for critical operations, such as enrollments and account recovery.		✓
5.6	MSTG-NETWORK-6	The app only depends on up-to-date connectivity and security libraries.		✓

MASVS: Network

Security Verification Requirements

#	MSTG-ID	Description	L1	L2
5.1	MSTG-NETWORK-1	Data is encrypted on the network using TLS. The secure channel is used consistently throughout the app.	✓	✓
5.2	MSTG-NETWORK-2	The TLS settings are in line with current best practices, or as close as possible if the mobile operating system does not support the recommended standards.	✓	✓
5.3	MSTG-NETWORK-3	The app verifies the X.509 certificate of the remote endpoint when the secure channel is established. Only certificates signed by a trusted CA are accepted.	✓	✓
5.4	MSTG-NETWORK-4	The app either uses its own certificate store, or pins the endpoint certificate or public key, and subsequently does not establish connections with endpoints that offer a different certificate or key, even if signed by a trusted CA.		✓
5.5	MSTG-NETWORK-5	The app doesn't rely on a single insecure communication channel (email or SMS) for critical operations, such as enrollments and account recovery.		✓
5.6	MSTG-NETWORK-6	The app only depends on up-to-date connectivity and security libraries.		✓

MSTG Network

App Transport Security (MSTG-NETWORK-2)

Overview

App Transport Security (ATS) is a set of security checks that the operating system enforces when making connections with NSURLConnection, NSURLSession and CFURL to public hostnames. ATS is enabled by default for applications build on iOS SDK 9 and above.

ATS is enforced only when making connections to public hostnames. Therefore any connection made to an IP address, unqualified domain names or TLD of .local is not protected with ATS.

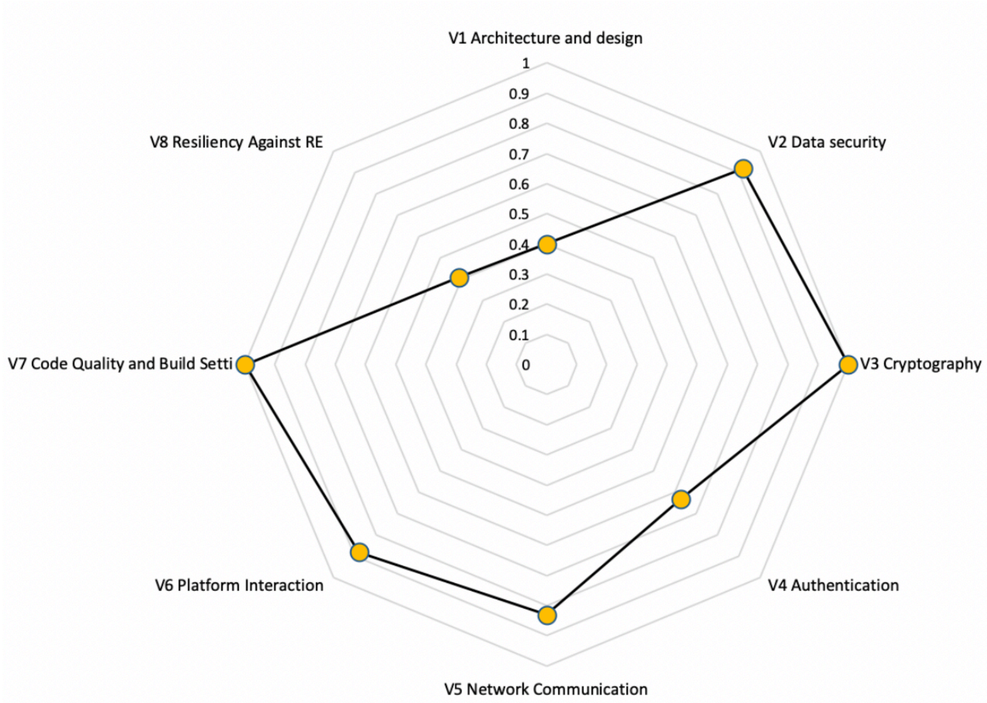
The following is a summarized list of App Transport Security Requirements:

- No HTTP connections are allowed
- The X.509 Certificate has a SHA256 fingerprint and must be signed with at least a 2048-bit RSA key or a 256-bit Elliptic-Curve Cryptography (ECC) key.
- Transport Layer Security (TLS) version must be 1.2 or above and must support Perfect Forward Secrecy (PFS) through Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) key exchange and AES-128 or AES-256 symmetric ciphers.

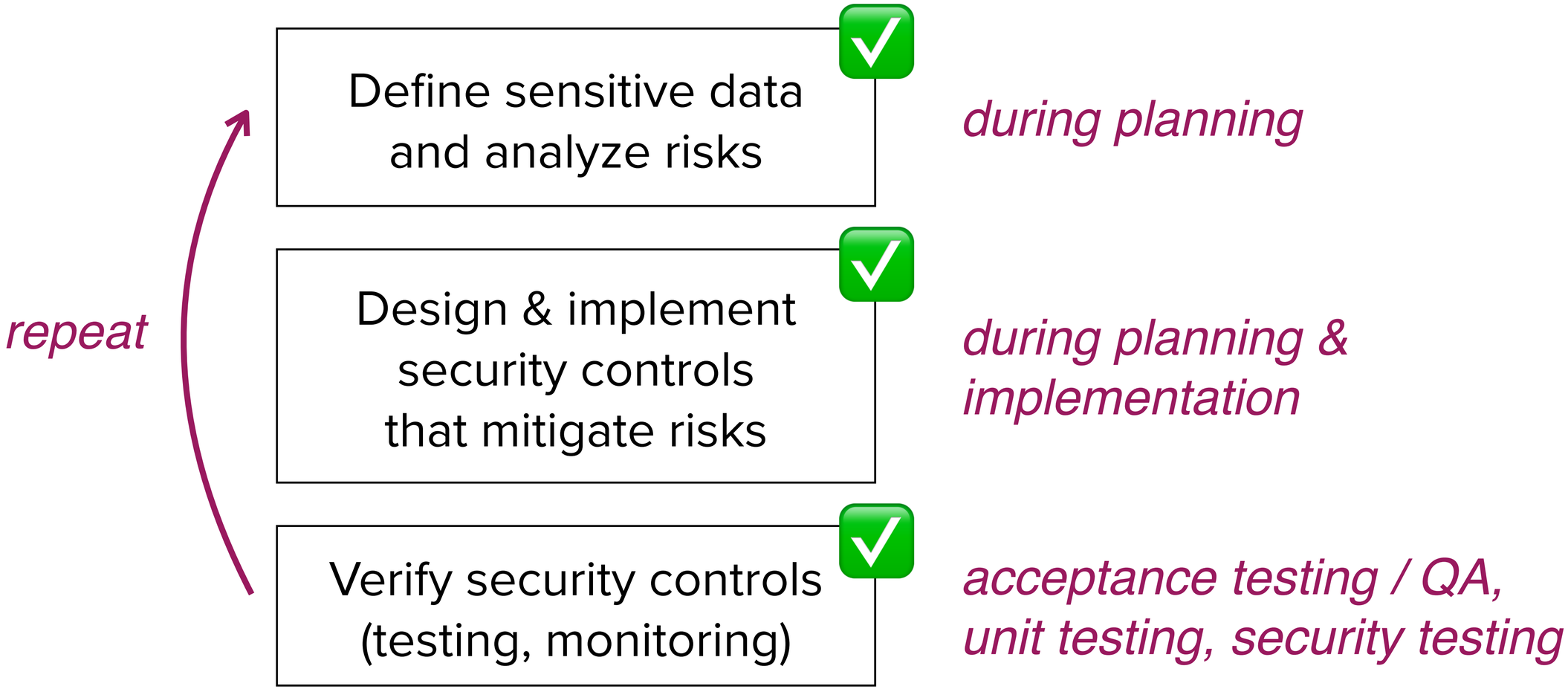
The cipher suite must be one of the following:

- `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384`
- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA`
- `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256`

— Use MASVS+MSTG to calculate “security scores” and improve them long term.



SSDLC in simple words



SSDLC is easier together

Define sensitive data and analyze risks	*defining organization's cybersecurity program, risk assessment, compliance mapping*
Design & implement security controls that mitigate risks	*designing security architecture, security engineering, building cryptographic schemes*
Verify security controls (testing, monitoring)	*accessing and verifying controls, code audits, app sec audits, pen testing, security monitoring*


Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Identity Management
Privileged Access Management
Identity & Access Management
Security Engineering
Cryptography
Framework and Standard
COBIT
ISO/IEC
SANS/CSC
NIST
Career Development
Certification
Training
Conferences
Peer Groups
Self Study
Physical Security
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Penetration test
Blueteam
Social Engineering
Redteam
Application
Infrastructure
Source Code Scan
Blackbox
Whitebox
Data-Centric Risk Assessment
Data-Flow Map
Governance
Laws and Regulations
Industry Specific
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
KPIs/KRIs
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
Policy
Procedure
Guideline
Standard
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Eradication
Investigation
Forensics

available in workbook

Workbook time!

Thank you!

feedback form

https://forms.gle/WcoFhV4t5ehLDbhm8

Anastasiia Voitova

ping me if you're interested in more deep-dive workshops/trainings, or in app security engineering assistance.

@vixentael

anastasi@cossacklabs.com