Microsoft

Secure DevOps: Application Security Principles and Practices

Module:
Policy, Standards and Compliance

Microsoft Services

Warning!

- None of this should be considered legal advice nor compliance advice
- Do not, under any circumstances, imply that this work will confer compliance

Module Overview

- Lesson: Policies and Standards
- Lesson: Understanding Compliance
- Lesson: Threat Modeling for Compliance

Lesson: Policies and Standards

“The good thing about standards is that there are so many to choose from.”

— Andrew S. Tanenbaum

Standards

- As noted, there’re many standards and many relate to security
- Examples include:
  - S/MIME, X.509, RFC 2898, TLS 1.x, FIPS 140-2, NIST 800-53 etc.

- Standards help provide a baseline level of acceptance and interoperability
- If TLS were not standardized, web servers and web browsers would not interoperate

OWASP Top 10:
A Common Baseline Security Standard

- The OWASP Top 10 is a well-known way to get to a secure baseline
- It's not uncommon for customers to demand systems that adhere to Top 10 practices
- It's a low, but practical bar
- https://owasp.org/Top10/

OWASP Top 10 Practicalities

- All developers and architects should attempt to prevent or remediate the OWASP Top 10 issues
- Different SDL practices can find/mitigate various OWASP issues
- There is overlap between some OWASP items

Alternatives to the OWASP Top 10

- The most common alternative is the CWE/SANS Top 25
- CWE is the Common Weakness Enumeration and is a comprehensive list of security vulnerabilities
- CWE/SANS Top 25 is not updated often enough, however
- The CWE itself is a well-known ‘standard’ for vulnerability classes
  - It’s a great way to express a vulnerability
  - Commonly used on code review and pen-test results

Internal Security Standards

- At a minimum, you should have standards around:
  - End-to-End design, development and testing practices
  - Cryptography
  - Tools use
  - Programming standards
- It's critical you understand how compliance programs impact your solution
  - GDPR, SOC, PCI etc.

End-to-End Practices

- This is why the SDL exists!
- You must define security-related practices
- Start with the SDL, and use appropriate tasks as needed
- At a minimum use:
  - Education
  - Threat modeling
  - Static analysis

Cryptographic Standard

- Incredibly important
- You need to define standards for:
  - Key sizes
  - Symmetric Algorithms
  - Asymmetric Algorithms
  - Hashing
  - MACing
  - Block-cipher modes
  - Signatures
  - Key generation
  - Secret storage

The Microsoft Cryptographic Standard

- Symmetric Algorithms
  - AES is, by far, the preferred algorithm
  - 128-bit key size minimum
  - No ECB (Electronic code book)
  - CBC (cipher-block chaining) or GCM (Galois Counter Mode)
  - RC4, DES, RC5 explicitly banned
  - Exceptions granted for 3DES for compatibility
- Asymmetric Algorithms
  - RSA 1024 minimum
  - Elliptic Curve (ECC)

The Microsoft Cryptographic Standard

- Hashing
  - SHA-256+
  - Exceptions granted for SHA-1 for compatibility
- Message Authentication Code (MAC)
  - Must use a secure base algorithm, for example SHA-256
- Key Generation
  - Must use an approved standard (FIPS 186-2) generator
  - Must derive keys from passwords using RFC 2898 (or better) algorithms
- Secret Storage
  - Hardware where possible, OS-based defenses otherwise

Tools Usage

- This would define which tools and options to use in the development tool chain
- For example:
  - Compiler version
  - Compiler/linker flags
  - Static analysis tool(s)
  - Dynamic analysis tool(s)

Programming Standards

- This should be a short, readable and practical document that explains the minimum secure coding bar
  - No embedded keys/passwords
  - No C# code marked ‘unsafe’
  - No unsafe C functions (strcpy, strcat etc.)
  - All input is verified for correctness using regex
  - All HTML output is encoded
  - Etc.

Open-Source Policy

- Not security related
- Critically important, however
- You need a policy around:
  - 1) which OSS licenses you will accept (GPL? MIT? Apache?)
  - 2) how you license any source you share (eg; Github)
- Be aware of the implications of certain licenses
- Adding GPL code to your code makes it GPL code

Handling Security Issues

- You need a policy that explains how you will handle a security vulnerabilities reported to you and issues you find in other products
- Coordinated Disclosure is the policy de-jour.
  - https://www.microsoft.com/en-us/msrc/cvd

Discussion

- What compliance and standards does your organization adhere to?

Lesson: Understanding Compliance

Compliance Programs

- Compliance is important to customers
- Compliance can help drive security
- For some, compliance == security
- Sadly, compliance != security
  - Many PCI-compliant merchants have been compromised
  - Many HIPAA-compliant healthcare providers have been compromised

Azure Compliance

- Azure Trust Center offers plenty of guidance about numerous compliance programs
  - https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx
- It should be the first port of call
- All Azure subscribers can access Azure compliance audit reports

Standards you Should Know About

- GDPR
- HITRUST
- HIPAA
- FedRAMP
- PCI DSS 3.2.1
- Cloud Security Alliance CCM
- FIPS 140-2
- NIST 800-53
- ISO 27034
- SOC

GDPR

- European Union's General Data Protection Regulation
- Came into effect early 2018
- Focus on user privacy and security
- Steep fines for non-compliance

I – General provisions
II – Principles
III – Rights of the data subject
IV – Controller and processor
V – Transfers of personal data to third countries or international organizations
VI – Independent supervisory authorities
VII – Cooperation and consistency
VIII – Remedies, liability and penalties
IX – Provisions relating to specific processing situations
X – Delegated acts and implementing acts
XI – Final provisions

HITRUST

- Focus on healthcare
- A ‘meta’ compliance program
  - It maps to other programs like HIPAA, SOC, GDPR

0. Information Security Management Program
1. Access Control
2. Human Resources Security
3. Risk Management
4. Security Policy
5. Organization of Information Security
6. Compliance
7. Asset Management
8. Physical and Environmental Security
9. Communications and Operations Management
10. Information Systems Acquisition, Development and Maintenance
11. Information Security Incident Management
12. Business Continuity Management
13. Privacy Practices

HIPAA

- Health Insurance Portability and Accountability Act
- In effect since 1996
- Focus on healthcare
- A big update is in the works, with a large focus on tech

FedRAMP

- US Federal Risk and Authorization Management Program
- Focus on cloud security
- Goal is to help Federal agencies move securely to the cloud
- Ever wonder why there're US Govt Azure data centers?
- Three levels: High, Moderate and Low
  - Higher levels have more security controls

PCI DSS

- Payment Card Industry Data Security Standard
- A response to insecure credit card merchants
- Not perfect, but generally well-respected

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

Cloud Security Alliance Cloud Controls Matrix

- Another “Meta-Program”
- Focus is on cloud providers
  - but it’s of use outside of cloud providers
- Documentation is approachable and practical
- Includes a reverse mapping to other compliance programs

FIPS 140-2

- Federal Information Processing Standards
- FIPS 140-2 focuses on approved cryptographic implementation
- Level 1 – 4, with increasing rigor and trustworthiness

NIST 800-53

- National Institute of Standards and Technology
- Security Controls and Assessment Procedures for Federal Information Systems and Organizations

Control Families

AC - Access Control
AU - Audit and Accountability
AT - Awareness and Training
CM - Configuration Management
CP - Contingency Planning
IA - Identification and Authentication
IR - Incident Response
MA - Maintenance
MP - Media Protection
PS - Personnel Security
PE - Physical and Environmental Protection
PL - Planning
PM - Program Management
RA - Risk Assessment
CA - Security Assessment and Authorization
SC - System and Communications Protection
SI - System and Information Integrity
SA - System and Services Acquisition

ISO 27034

- "ISO/IEC 27034 offers guidance on information security to those specifying, designing and programming or procuring, implementing and using application systems"
- Annex A maps the Microsoft SDL to ISO 27034

A.12 SDL mapped to the Application Security Life Cycle Reference Model

In the interest of reader clarity, the SDL process can be mapped to the Application Security Life Cycle Reference Model diagram included in ISO/IEC 27034. Reference Model stages covered by the SDL process are printed in bold in Figure A.6.

https://sdl.ssg.gov.sg/DOCs/Annex_A_SDL_FAQ.pdf

SOC

- Service Organization Control
- There’re three versions 1, 2 and 3
- SOC 1 focuses on financial controls
- SOC 2 and 3 focus on security, processing integrity, confidentiality, or privacy of a data center's system and information
- SOC 2 and SOC 3 offer the same results, but SOC 3 is smaller and aimed at a more general audience, SOC 2 is for stakeholders

Demo: Compliance

Show the CSA CMM documentation and cross-reference

Lesson: Threat Modeling for Compliance

Using Threat Models to Help Drive Compliance

- Compliance programs often have various over-arching section:
  - Physical
  - Management
  - Technical
- There's little anyone in this room can do about the first two
- The third, technical, we have full control over
- What if we could give compliance auditors something that shows we have the technical controls in order?

Using threat models to aid Compliance

- Threat models focus on mitigations (aka defenses, compensating controls)
- The technical portions of compliance programs also focus on mitigations
- This is our link
- Build out the threat model
- Map the defenses to the appropriate compliance program(s)
- This becomes an artifact we can hand to auditors

Example 1 – Database encrypts data at Rest

Maps to

PCI DSS Req 3

HITRUST 10.03

FedRAMP SC-13

Data at rest is encrypted using "Always Encrypted"

PCI Security Standards Council

Protect Cardholder Data

Requirement 3: ***Protect stored cardholder data***

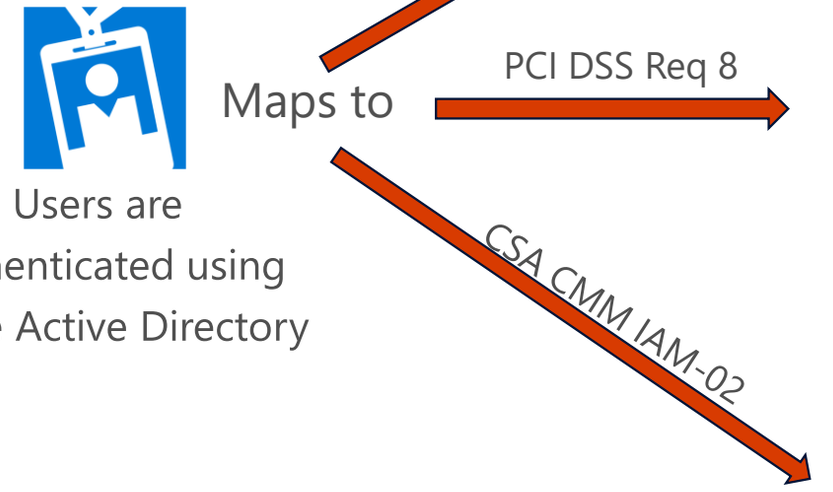
Protection methods such as encryption, truncation, masking, and hashing are critical components

Objective Name: 10.03 Cryptographic Controls

Control Objective:	To protect the confidentiality, authenticity and integrity of information by cryptographic means. A policy shall be developed on the use of cryptographic controls. Key management should be in place to support the use o

SC-13	CRYPTOGRAPHIC PROTECTION	The information system implements [As Supplemental Guidance: Cryptography information separation when authorized applicable cryptographic standards inclu other security controls, organizations de controls: AC-2, AC-3, AC-7, AC-17, AC-18 References: FIPS Publication 140; Web:

Example 2 – Authentication



Users are authenticated using Azure Active Directory

Maps to

FIPS 186 IA-2

PCI DSS Req 8

CSA CMM IAM-02

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Family: IA - IDENTIFICATION AND AUTHENTICATION
Class:
Priority: P1 - Implement P1 security controls first.
Baseline Allocation:

Low	Moderate	High
IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)

PCI Security Standards Council

Requirement 8: Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that each individual

CCM v3.0.1

Control Domain	CCM V3.0 Control ID
Identity & Access Management Credential Lifecycle / Provision Management	IAM-02

Demo: Threat Modeling and Compliance

Show a real threat model mapped to HITRUST

Knowledge Check

- Name some of the compliance standards
  - GDPR
  - HITRUST
  - HIPAA
  - FedRAMP
  - PCI DSS 3.2.1
  - Cloud Security Alliance CCM
  - FIPS 140-2
  - NIST 800-53
  - ISO 27034
  - SOC

Module Summary

- Policies and Standards are good
- Compliance can help drive improvements in security
- High-level overview of some current standards
- The Threat Modeling process can improve compliance

Security Practices – Secure DevOps

Assume breach

Design for failure

Auto/Proactive

Secure DevOps

Feedback Loop & Continuous Improvement

Business Ideas → Ideas Discussed → Reqs/NFR Created → Architecture Defined → Design Specified → Develop & Unit Test → Build & Integrate → Function & NF Test → Staging & UAT → Deploy to PRD → Operate & Support


Customer Trust


Governance Compliance


GDPR/MAS Regulation


Secure Architecture

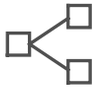

Threat Modeling

App&OSS Testing


Secure Infra/Data


Security Testing


Red/Blue Teams


Identity Access


DevSecOp Collaboration


Culture, Mindset, New Structure & Collaboration


Learning, Education, Skills & Champions


Automation & Shift-Left Security Testing & KPI Dashboards