Secure Product Lifecycle

Introduction and Overview

Winter 2024/2025, 705.070 VO; 705.071 KU

Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

Today‘s Agenda

- Who we are, Yagoba GmbH & SGS
- Organizational Overview
  - LV - Lecture Content
  - KU - Content and Modus
- Secure Product Lifecycle - Introduction

Yagoba

- Yagoba is a SME based in Graz
- More then 50 years of practical experience in secure application development and certification
- Projects from secure banking application, via secure automotive applications to test tools

Organisational Overview

LV

- 10 lectures covering aspects within a product life cycle
- Every wednesday, 12:15-13:45 (check online for changes)
- Written exam at the end of the semester

KU

- Apply methodologies discussed in the lecture in small exercise
- No exam, continuous assessment
- Details in first KU lecture

Communication

Best via Email:

- Christoph Herbst christoph@yagoba.com

- Discord: #spl for KU

LV Timetable

	Topic	Date	Time	Lecturer
	Introduction & Overview	09.10.2024	12:15-13:45	Christoph Herbst
1	**Risk Analysis & Threat Modeling**	16.10.2024	12:15-13:45	Christoph Herbst
2	**Secure Design & Requirements Management**	23.10.2024	12:15-13:45	Karin Maier
3	**Security Testing**	30.10.2024	12:15-13:45	Karin Maier
4	**Fuzz Testing**	06.11.2024	12:15-13:45	Srđan Ljepojević
5	**Penetration Testing: Web and Mobile App**	13.11.2024	12:15-13:45	Tomislav Nad
6	**IoT and Device Security Testing**	20.11.2024	12:15-13:45	Christoph Herbst
7	**Security Testing: Implementation attacks**	27.11.2024	12:15-13:45	Christoph Herbst
8	**Conformity assessment**	04.12.2024	12:15-13:45	Christoph Herbst
9	**Security from release to decommissioning**	11.12.2024	12:15-13:45	Christoph Herbst
	Exam	**29.01.2025**		

KU Timetable

Exercise	Start	Time	Submission	Lecturer
Threat modeling and risk analysis	21.10.2024	13:00-14:00	11.11.2024	Christoph Herbst
Security requirements document	11.11.2024	13:00-14:00	09.12.2024	Christoph Herbst
Security review	09.12.2024	13:00-14:00	06.01.2025	Christoph Herbst
Gate review	**Doodle 9.1.2025**			

Introduction to the

SECURE PRODUCT LIFECYCLE

Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

Motivation

- Security is not only a matter of technology
- Security needs to be considered over the full product lifecycle
- Relevant security standards like Common Criteria, ISO 62443, etc consider the full lifecycle

- This lecture should close the gaps in teaching

Average cost of a data breach

3.62 Million USD in 2017

4.88 Million USD in 2024

https://www.ibm.com/reports/data-breach

https://pixabay.com/photos/bank-notes-dollar-us-dollars-usd-941246/

Security Misconception

Security should not be a matter of fences…

https://pixabay.com/photos/fence-metal-fence-spikes-protection-7454135/

Security Misconception

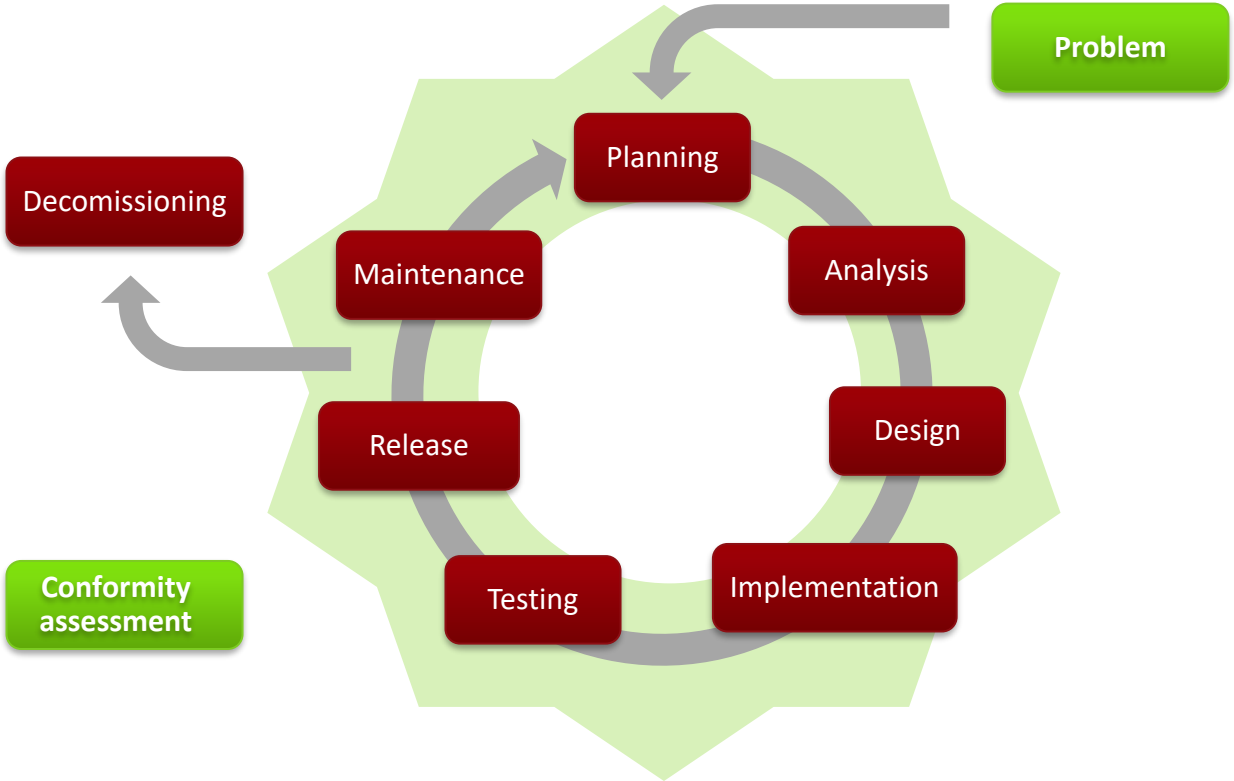
https://pixabay.com/photos/electrician-wiring-mounting-tool-3087536/

…or products or tools

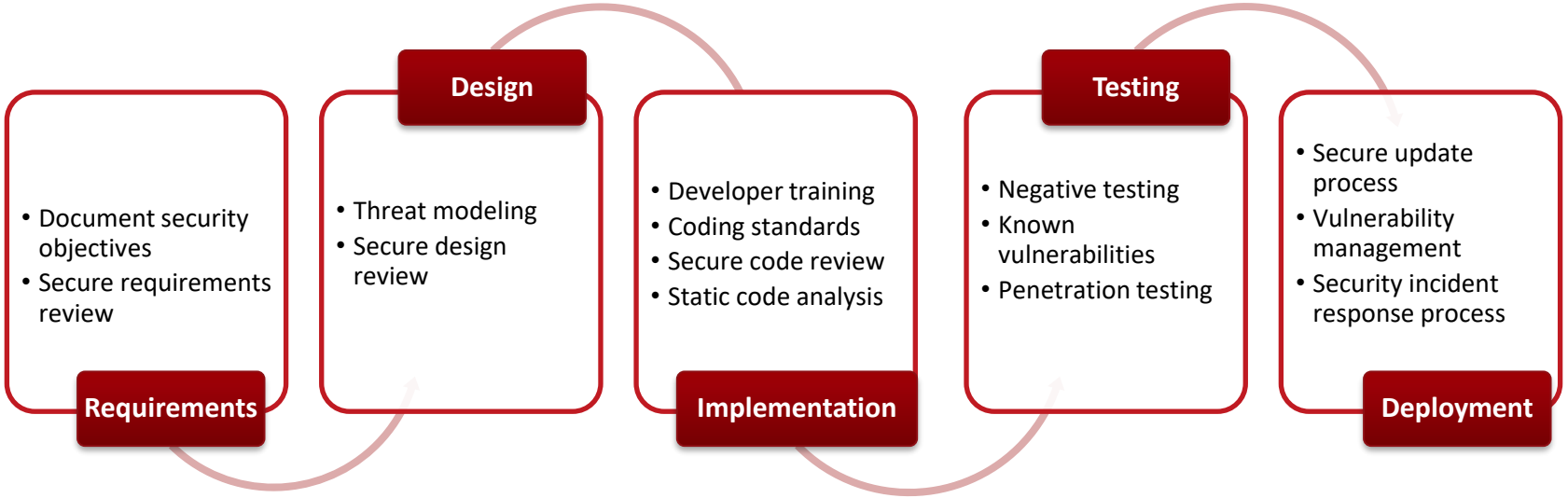
Key Principles

- Security should be a process
- Security should be testable
- Security should be measurable
- → Security must be integral part of a product’s lifecycle

Secure **Product** Lifecycle



Secure **Development** Lifecycle



Life Cycle Stage

PLANNING

Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

Planning

- Development process plan
- Deliverables (incl. documentation) of activities & tasks
- Traceability between requirements, test & risk control
- Software configuration & change management
- Problem resolution for handling problems detected in software products

Cost of bug fixing or security implementation depending on phase security is added to lifecycle (IBM Research, NIST)

*X is a normalized unit of cost and can be expressed in terms of person-hours, dollars, etc.
Source: National Institute of Standards and Technology (NIST)

Planning: Best Practices

- Plan and ensure all stakeholders are aligned with the goals and responsibilities
- Execute and action on planning changes
- Re-evaluate initial planning often, in sync with lifecycle stages
- Assign security architect role for development

Life Cycle Stage

ANALYSIS

Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

Analysis

- Security should be considered from the ground up
- Include security in the requirements
- Include regulatory requirements
- Risk and threat analysis to understand
  - Business risks of successful exploits
  - Costs of liability, redevelopment, and damage to brand image and market share

Analysis: Best practices

- Document key security objectives
- Separate security requirements from functional requirements
- Establish traceable requirements for upcoming lifecycle stages
- When defining what a system must do, also consider what a system must not do
- For every use case, write misuse case (intentional misuse)
- Consider DoS scenarios
- Write requirements for industry standards & regulatory rules

Life Cycle Stage

DESIGN

Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

Secure Design

- Define threats to a system in a detail that allows developers to understand and code against
- System architecture should mitigate as many threats as possible
- Component level security to be considered
- Design techniques that force developers to consider security with every line of code they write
- Lifetime security

Secure Design: Best practice

- Threat modeling
- Design techniques that mitigate risks
- Identify components essential to security – components that perform
- Provide developer security guidelines
- Establish a security test plan (independent of functional tests)
- Plan for incident response (expectations of perfect security are unrealistic – effort/money)

Life Cycle Stage

IMPLEMENTATION

Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

Implementation

- Focus on security in the requirements and design phase sets the stage for writing secure code
- Mistakes can still occur – code is developed by (imperfect) humans
- Follow secure implementation best practices and ensure that best practices are up to date

Implementation: Best practices

- Secure coding guidelines
- Code review & guidelines
- Automated static code analysis
- Defect management
- Retest security defects
- Re-review and retest all security fixes

Life Cycle Stage

TESTING

Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

Testing

- Include security testing into test concept
- Test 3rd party components for known vulnerabilities & weaknesses
- Perform automated security tests
- Perform penetration tests
- Consider customer environment during testing

Testing: Best practices

- Positive and negative testing
- Unit testing for security
- Static code analysis
- Static binary analysis
- Dynamic analysis
- Known vulnerability scanning
- Penetration testing
- Deployment and integration testing

Life Cycle Stage

RELEASE

Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

Release

- Ensure you build what you intend to build
- Test the release
- Traceability of release to requirements
- Ensure updatability of release
- Secure shipment procedure

Release: Best Practice

- Configuration Management in place
- Follow a Secure Release Process
- Your software will need a Secure Update Process
- Consider Long-Term Security

Life Cycle Stage

MAINTENANCE

Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

Maintenance

- Vulnerability management
  - For 3rd party products
  - For own product
- Understand existing infrastructure of an application & maintain documents to match changes being made
- Predefined timelines
- Secure update process
- End user notifications
- Secure logs for security relevant events

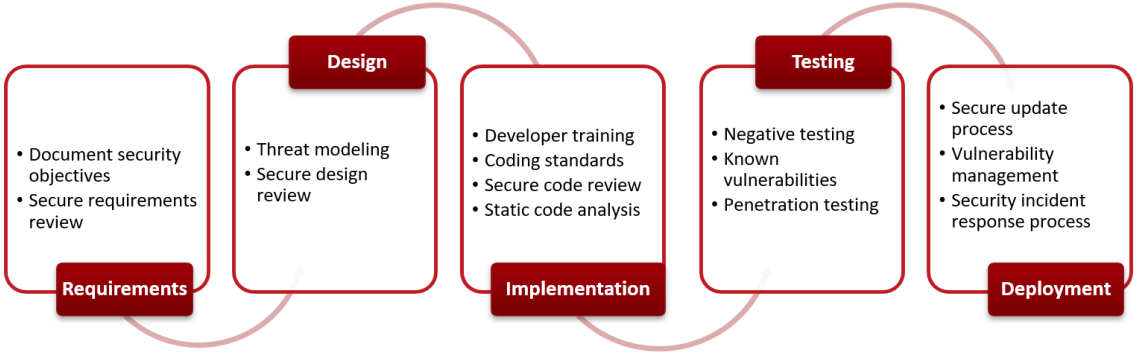
Maintenance: Best Practices

- Patches & fixes shall be developed following same lifecycle
- Have a development environment that supports fast and reliable builds and automated testing
- Roll-backs shall be considered for unsuccessful/faulty patches
- Incidence response plan

SUMMARY

Secure Product Lifecycle

- Security is a process
- Security must be considered in every phase of the development lifecycle



- Must be considered by all involved
  - Developers
  - Testers
  - Managers

KU Preview

- Groups of 3 people
- Secure Access Control system
  - Phone or token, Door, Backend
- Tasks
  - Detail your deployment environment
  - Threat and Risk analysis
  - Requirements establishment
  - Review

- More details will follow in the first KU lecture, 21.10.2024 13:00