Product Cyber Security

Reflections from an implementation & development perspective

Kenneth Solberg, Technical Lead Connectivity, Ship Intelligence

January 2019

01

Developing Product Cyber Security

Comparison of Product and Enterprise Security

Requirements Sources

Risk

Implementation

Product Security

Comparison

Product vs Enterprise Security

Product Security

- Products are changing with through formal process
  - System behavior is «fixed»
- Products and systems are not easily accessible
  - Poor connections (satellite or similar)
  - Traditionally isolated
- Different roles in the organisation with different skills are supporting the system whenever needed.
- Requirements are driven by
  - Safety
  - Production/uptime
- Compliance with Maritime environment

Enterprise Security

- Network and nodes and applications can change on a daily basis
  - System behaviour can change
- Systems are easily accessible
  - Direct connections
  - 24/7 Connections
- Highly skilled dedicated engineers are monitoring and changing the systems on a daily basis
- Business changes drive requirements
- Non compliance with maritime environments

Product Security

Comparison

Product vs Enterprise Security Cont.

- Security Governance Structures
- Processes
  - Ie. Escalation and response times
- Research & Development
  - Requirements
  - Design
  - Implementation
  - Testing
  - Release
- Maintenance and lifecycle
  - Upgrades and patching
  - Patching strategies
- DevOps
- Security Systems
  - Intrusion Detection and Prevention
  - Security Operation Centers

Requirements Sources

Sources of Requirements

- General Data Protection Regulation
- Customer Requirements
- 3rd party actors
  - Integration with 3rd party actors
  - Embedding 3rd party components
- Company / Corporate standards
- Insurance Companies
- Regulatory bodies

Product Security

Requirements Sources

Security Standards and Guidelines

- ISM
  - 2018 ISM Code - Cyber Security Appendix (IMO MSC-FAL.1-Circ.3 - Guidelines On Maritime Cyber Risk Management)
- ISO/IEC
  - ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements
  - ISO/IEC 27002:2013 Information Technology-Security Techniques-Code of Practice for Information security controls
  - IEC 62443-3-3 Industrial communication networks — Network and system security Part 3-3- System security requirements and security levels
- ISA
  - ISA 62443-1-1 Security for Industrial Automation and Control Systems Part 1
  - ISA 62443-4-1 Security for Industrial Automation and Control Systems Part 4
- NIST
  - NIST Cybersecurity Framework -Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (April 2018)
  - NIST SP 800-12 An Introduction to Information Security
  - NIST SP 800-30 Guide for Conducting Risk Assessments
  - NIST SP 800-39 Managing Information Security Risk- Organization, Mission, and Information System View
  - NIST SP 800-68 Guide to Securing Microsoft Windows XP Systems for IT Professionals- NIST Security Configuration Checklist
  - NIST SP 800-82 Guide to Industrial Control Systems Security

Product Security

Requirements Sources

Security Standards and Guidelines cont.

- USCG Maritime Bulk Liquids Transfer, Offshore Operations, and Passenger Vessel Cybersecurity Framework Cybersecurity Framework Profiles (2017)
  - Cybersecurity Framework Profiles Overview
  - Appendix A. Maritime Bulk Liquid Transfer Profile
  - Appendix B. Offshore Operations Profile
  - Appendix C. Passenger Vessel Profile
  - Appendix D. Industry Cybersecurity Processes & Profile Mappings
- Guidelines on Cyber Security Onboard Ships (BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI)
- API Security Guidelines for the Petroleum Industry
- API Security Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries
- NOG 104 Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control,safety and support ICT systems
- ABS Cybersecurity Guide Volume 1 and Volume 2
- LR
  - LR Cyber Enabled Ships ShipRight Procedure
  - LR Guidance Note Cyber Enabled Ships
- DNVGL
  - DNVGL RP-0496 Cyber security resilience management for ships and mobile offshore units in operation
  - DNVGL-RP-G108 Cyber security in the oil and gas industry based on IEC 62443

Product Security

Requirements Sources

Key messages

Understand which requirements sources are relevant for your product and business.

Communicate this transparently internally and to your customers

Security need to be addressed wholistically, such that the implementation of security is essential at all levels in your organisation!

Do not create any processes or policies unless there is an understanding on how it shall be successfully implemented into the organization!

Security Overview

Risk and Impact

Risk Awareness

- Have you followed an industry wide risk capture process?
- What is your perception of a risk?
- Are risks transparently communicated to relevant stakeholders?
- Who owns the risks in your organisation and customer?
- Are risks assessed and properly mitigated?
- What is your risk appetite?

Risk Impact

- Costs
  - Damage to property
  - Operations
  - Competitivness
- Reputational damage
  - Competitivness
- Safety
  - Current Operations
  - Future Operations

Security Overview

Risk and Impact

Key Message

Understand the driving forces of the security related decisions which you make in your organisation!

Risk owners must take ownership through ensuring that mitigations are properly implemented and residual risk is thoroughly communicated

Product Security

Implementation

Governance Frameworks and Processes

- Secure Development Lifecycle (SDL)
- NIST Cyber Security Framework
- ISO and DNV-GL
- Building Security In Maturity Model

Implementation of Secure Development Lifecycle

"In its simplest form, the SDL is a process that standardizes security best practices across a range of products and/or application", *Techbeacon.com*

«*Secure Development Lifecycle* is a different way to build products; it places *security* front and center during the product or *application development* process. From requirements to design, *coding* to test, the SDL strives to build *security* into a product or *application* at every step in the *development* process", *Techbeacon.com*

Product Security

Implementation

Implementation of Secure Development Lifecycle

- A risk based approach will allow to focus on product areas which adds most value
- Involve all levels in the organisation
  - Make the rationale and the risks clear for all levels in the organisation
  - Distribute responsibilites to ensure ownership
    - Security Champions?
- Continous evaluation and assessments
  - Communicate why activitites are being done.
- Lower the barrier to perform security related activities
  - «Everyone in the organisation shall be able to perform activitites that enhances security that is applicable to their level in the organisation»

Product Security

Implementation

Security Validation & Verification Activities

- Peer review
  - Configurations
  - Code
  - Design changes
- Static code analysis tools
- By Design
- Processes
- Pentesting
- Etc.

Secure Integration

- How to implement a secure integration?
  - Availability
  - Integrity
  - Confidentiality
  - Authentication
  - Non-repudiation
- Which security solutions to apply?
  - What need to be mitigated and how much risk can be tolerated?
- Assume that any other system is compromised and treat it likewise
  - By design, by process

Product Security

Implementation

Key Messages

- Keep it simple, increased complexity increases the threat surface
- Choose a security framework for your organisation
  - Implement it across the whole business
- Continuous training
  - Not a one-time event
- Lower the barrier for any role to validate and verify the security stance throughout the whole product lifecycle

03

Dilemmas

Dilemmas and Open Questions

Key messages

Dilemmas

Dilemmas and Open Questions

1) Product is sufficiently secured and risks are accepted. A last minute change is challenging the security. What do you do?

2) The added security measures has increased the cost such that the product has reduced competitivness. What do to?

3) How much is it expected that the company shall invest in Cyber Security?

4) How can you know if you are sufficiently secured?

Key messages to resolve the dilemmas

- Understand the risks associated with your products and the impact to the business
  - Manage these risks according to the “As Low As Reasonable Practicable” principle
- Ensure that a person who understands and is capable of presenting security related risks is a part of the executive group
  - Risks need to be understood and communicated adequately to the right stakeholders, since it can have severe impact to the business if not sufficiently mitigated.
- Create response/escalation methods and perform related training
  - All levels in the organization

Challenge

«How can YOU use your role to make your products more secure»


ROLLS
ROYCE