A holistic approach to ensure product security

Christer Stenhäll
Ericsson PSIRT
Agenda

— Ericsson at a glance
— Our perspective on Security
— SRM, this is how we do it
— PSIRT
— Vulnerability Management
— Conclusion— Next Steps
Ericsson at a glance

Enabling the full value of connectivity for service providers

Business areas:
- Networks
- Digital services
- Technology and emerging business
- Managed services

By the numbers:
- 180+ countries
- 201.3 b.sek in sales
- 100,700 employees
- 45,000 patents
Our perspective on Security in the networked society

- services should always be available
- security should require minimum effort from users
- communications should be protected
- all access to information and data should be authorized
- manipulation of data in the networks should be possible to detect
- the right to privacy should be protected
Building Trust

- TRUSTED BUSINESS: Business decision to accept residual risks and manage unacceptable risks
- TRUSTED Operations: Appropriate procedures for secure operations
- TRUSTED Network: Sound, manageable security architecture
- TRUSTED Products: Devices/nodes/products without exploitable vulnerabilities

Driving & contributing to improving standards
Security Reliability Model (SRM)
Baseline Requirements & Design Rules

Baseline Security & Privacy Requirements
  • both functional and non-functional requirements

Security and Privacy Design Rules
  • How to implement requirements
Security Functionality areas

Security functions divided into **6 areas** based on the defence in depth.

**Network Protection**
- Conf & integ protection of O&M, Server side authentication

**Application Security**
- Software Signing, Web application security

**Platform Security**
- Malware Prevention, Trusted state and secure boot

**Identity and Access Management**
- Enforce replacement of passwords, Support password aging

**Logging**
- Full Personal Accountability, Ability to Log Locally

**Data Protection**
- Password protection, Confidentiality and Integrity of Personal Data
Security Assurance
Security Reliability Model (SRM)
Security Assurance levels

- All of Ericsson Products
  - All mandatory assurance items and the basic security functionality
- Products with Special Security requirements
  - Tailored Assurance
- Products with Need of a High Security assurance
  - Advanced level
Security Assurance

- Risk Assessment
- Privacy Impact Assessment
- Secure Coding
- Vulnerability Assessment
- Vulnerability Management
- Hardening
Security Assurance RA

— RA for new products
  • Determine the appropriate security level
  • What security functions are needed

— RA in the end of development
  • Costly and difficult to make changes

— Risk Assessment in Development

— Risk Assessment report
  • Risk Identification
  • Risk Rating (severity)
  • Risk Treatment Plan

Privacy Impact Assessment

Secure Coding

Vulnerability Assessment

Identification – Mitigation – Verification

Risk Reporting

1. Pre-study
   - Plan RA
2. Design
   - RA Result
3. Conclusion
   - RA Conclusion
Privacy Impact Assessment

- Privacy Data Classification
  - What types of data does the product handle

- Privacy Information flows

- PIA for XaaS

- Privacy impact report
  - Description of the privacy impact (threats and related risks)
  - Existing privacy design features
  - Recommendations
Security Assurance SC

— Secure Coding Standard

— Education
  • Secure coding standard training for developers & testers
  • Up to date developer (programming) training
  • Continuous learning

— Static and Dynamic analysis

— Code review

— Secure Coding Report
Vulnerability Assessment (VA) normally done too late!

VA in Continuous Integration/Continuous Delivery (CI/CD)
- Developers are the Key
- Function testing done during development
  - Security testing
  - Verifying Hardening
Documentation
Security Reliability Model (SRM)
Security User Guide
Describes the security operation and maintenance activities that can be performed for the product

Security Test report
Test Report for external communication

Hardening Guideline
Instruction of tailored hardening to be done during delivery

RA / PIA Report
Report of identified security and privacy risks for internal use.

VA Report
Test Report for internal communication

Secure Coding Report
Describes the Security Coding activities done during the development
Services
Security Reliability Model (SRM)

Functions  Assurance  Documentation

Product Development  Services
Services

Secure Deployment

Consultancy

Security Support

Security aaS
Reporting issues/vulnerabilities in Ericsson products

Vulnerability Management

Vulnerability
Triage
Alert
Answer
Vulnerability Database
Product Registration

Communication

Development
Conclusion

Next Steps

- SRM – Risk based approach
- Security awareness among developers are the key!
- Process transformation to be more lean & agile
- Improvement still needed on aSways of working
- Who to contact: psirt@ericsson.com