NOKIA

Nokia Networks

ensuring security

the way how we do it

HUSTEF, 2015.11.18

Attila Tóth

Disclaimer

The ideas, processes, tools are presented from a practitioner’s point of view working on a specific Nokia product. This presentation aims to give an insight, but does not attempt to reach detailed and full coverage valid for all Nokia products.

Basic principles

- **Confidentiality**: no information disclosure to 3rd party
- **Integrity**: information / data / piece of code has not been manipulated or altered
- **Authentication**: ensuring that parties involved are those who they claim to be
- **Availability**: service / data is available when required
- **Authorization**: parties have the authority to perform the action
- **Non-repudiation**: when sending data / message, the party cannot claim later that it was not him who sent it

Methods and layers to test security aspects in Nokia

Static testing

Dynamic testing

Methods and layers to test security aspects in Nokia

Static testing

- Threat and ris

Threat and risk analysis

- Organized as a workshop and documented
- People involved: software and test architects, lead testers and developers, product management
- We are looking for the answers for the following questions:
  - What are the assets that we need to protect?
  - Who are the potential attackers?
  - What are the potential attack scenarios?
  - What are the likelihood of these attacks?
  - What is the impact?
  - What can we do to reduce the likelihood or impact?

Methods and layers to test security aspects in Nokia

Static testing

- Threat and risk analysis
- Privacy assessment

Privacy risk assessment

- Privacy sensitive data:
  - anything that can be used to track and identify a certain individual
  - can potentially be used for abusing privacy rights.
- Assess each piece of data generated / processed / stored

Methods and layers to test security aspects in Nokia

Static testing

- Threat and risk analysis
- Privacy assessment
- Feature documentation review

Feature documentation review

- Check the design before implementation
- Check whether product meets customer security requirements

Methods and layers to test security aspects in Nokia

Static testing

- Threat and risk analysis
- Privacy assessment
- Feature documentation review
- Code reviews, static analysis

Code review, static analysis

- Check code created
- Check adherence to secure coding guidelines
- Should spot things like:
  - Buffer overflow
  - Goto fail ☺
- Create your checklist e.g.:
  - Correct cipher?
  - Correct key size?
  - Proper random number?
  - Sensitive information revealed, logged or leaked?
  - Any weak points?

Methods and layers to test security aspects in Nokia

Static testing

- Threat and risk analysis
- Privacy assessment
- Feature documentation review
- Code reviews, static analysis
- Vulnerability notification

Vulnerability notification

- Follow up on new vulnerabilities found in 3rd party software, e.g.
  - http://cve.mitre.org/
  - http://osvdb.org/
  - Security bulletins of vendors
  - Mailing lists
- Apply security patches proactively

Methods and layers to test security aspects in Nokia

Static testing

- Threat and risk analysis
- Privacy assessment
- Feature documentation review
- Code reviews, static analysis
- Vulnerability notification
- Statement of security compliancy

Statement of security compliancy

- Create a list of security base requirements that all products shall meet
- Measure the compliancy on each release
- The compliancy score should not decrease

Methods and layers to test security aspects in Nokia

Discovery test & Port scanning

- To cross check target IP addresses
- To verify in-host firewall and running services on the SUT
- Should match documentation
- Tooling e.g.:
  - nmap (open source)

Dynamic testing

- Discovery test & Port scanning

Methods and layers to test security aspects in Nokia

Vulnerability scanning

- To verify whether vulnerability notification and patching works
- Scan installed software for known vulnerable versions
- Tooling e.g.:
  - OpenVas (open source)

Dynamic testing

- Discovery test & Port scanning
- Vulnerability scanning

Methods and layers to test security aspects in Nokia

Robustness testing (Fuzzing)

- To stress test the external interfaces with invalid traffic and observe any crashes
- Tooling e.g.:
  - Sulley (open source),
  - Peach (community edition)

Dynamic testing

- Discovery test & Port scanning
- Vulnerability scanning
- Robustness testing (Fuzzing)

Methods and layers to test security aspects in Nokia

Web app / database testing

- To test the web application for
  - SQL injection
  - Cross Site Scripting (XSS)
  - Cross Site Request Forgery (CSRF)
  - …
- Tooling e.g.:
  - mitmproxy (opensource)
  - Fiddler (free)
  - w3af (open source)

Dynamic testing

- Discovery test & Port scanning
- Vulnerability scanning
- Robustness testing (Fuzzing)
- Web app / database testing

NOKIA

Methods and layers to test security aspects in Nokia

Penetration / exploratory testing

- To work like a hacker and break into the system
- To try scenarios, learn how the system works, try different scenarios, repeat.
- Tooling e.g.:
  - Kali Linux (open source)
  - Anything ☺

Dynamic testing

- Discovery test & Port scanning
- Vulnerability scanning
- Robustness testing (Fuzzing)
- Web app / database testing
- Penetration / exploratory testing

Methods and layers to test security aspects in Nokia

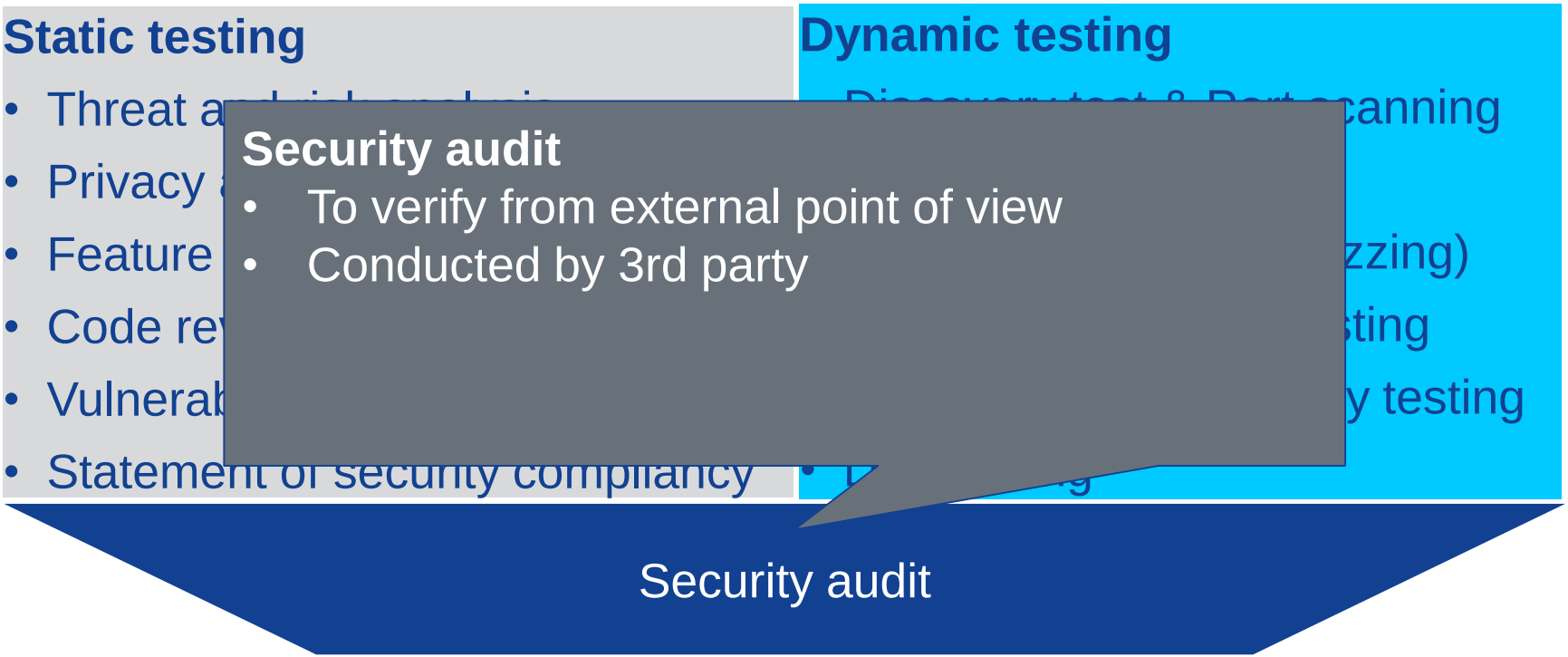
DoS testing

- To verify behavior under overload situation
- Tooling e.g.:
  - Performance verification test tool

Dynamic testing

- Discovery test & Port scanning
- Vulnerability scanning
- Robustness testing (Fuzzing)
- Web app / database testing
- Penetration / exploratory testing
- DoS testing

Methods and layers to test security aspects in Nokia



Methods and layers to test security aspects in Nokia

Static testing

- Threat and risk analysis
- Privacy assessment
- Feature documentation review
- Code reviews, static analysis
- Vulnerability notification
- Statement of security compliancy

Dynamic testing

- Discovery test & Port scanning
- Vulnerability scanning
- Robustness testing (Fuzzing)
- Web app / database testing
- Penetration / exploratory testing
- DoS testing

Security audit

NOKIA