Development and Industrial Application of Multi-Domain Security Testing Technologies

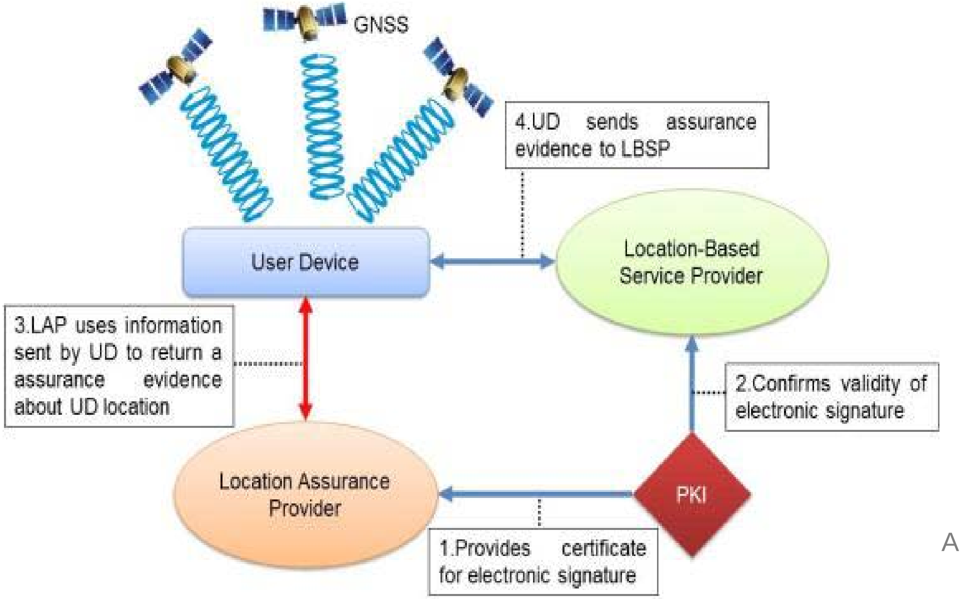
Case Study Experience Sheet
Localisation **A**ssurance **S**ervice **P**rovider (LASP)

Radio Protocol Case itrust

Case study characterization

Global Navigation Satellite Systems (GNSS) are becoming popular for everyone's use which is a vehicle for the emergence of services, called Location-Based Services (LBS). One problem is that the GNSS-like signals can be used without the users and LBS providers being able to assure that the location obtained is correct and has not been altered either intentionally or by mistake.

These security issues may hinder the current development of LBS in sensitive areas such as those related to protection against vehicle theft, accident reconstructions, alibi verification, monitoring the transportation of hazardous materials, etc.



GNSS

User Device

Location-Based Service Provider

Location Assurance Provider

PKI

1.Provides certificate for electronic signature

2.Confirms validity of electronic signature

3.LAP uses information sent by UD to return a assurance evidence about UD location

4.UD sends assurance evidence to LBSP

Radio Protocol Case itrust

Case study characterization

Security challenges:

1. Deny unauthorised access to LAP in a web services technology;
2. Prevent denial of service from mobile terminals by verifying efficiently XML structure.

Technical challenges:

1. Avoid errors in the mathematical model;
2. Improve performance of the LAP.

Radio Protocol Case itrust

Security testing approaches

Issue 1: Technical Audit

- For the purpose of security testing, itrust used the OWASP methodology; dedicated to testing the security of web applications.

The following test approaches were applied to the case study:

- Information gathering
- Configuration management testing
- Authentication testing
- Session management testing
- Authorisation testing
- Business logic testing
- Data validation testing
- Denial of service testing
- Web services testing
- Ajax testing

Radio Protocol Case itrust

Security testing approaches

Issue 2: Fuzzing tests

- Codenomicon provided us with about 10000 samples of fuzzing data for the user request content.

Issue 3: Unit testing

- We applied the testing methodology of Smartesting on the logical operations of the LASP software (i.e. management of user requests, user authentication, check of data sent by users).

Issue 4: Performance testing

- The performance testing was inspired by the “Performance Testing Guidance for Web Applications” published by Microsoft.

Radio Protocol Case itrust

Results and recommendations

Results

- 2 recommendations requiring an immediate action to avoid an inacceptable risk;
- 3 recommendations requiring a prompt action to avoid a high risk or prevent a certification;
- 5 recommendations requiring a dedicated action to reduce a medium risk or increase compliance.
- 3 recommendations requiring a dedicated action from relevant staff to avoid inconsistencies with documentation and non-compliance with what is expected.

Recommendations

- Put authentication on applications that don’t need to be public;
- Fix or remove snort report applications;
- Restrict access to the Tomcat manager.

Radio Protocol Case itrust

Results and recommendations

Fuzzing testing

- The samples were tested on the LAP server and results showed that the LAP server correctly caught Exceptions created by malformed user request content.

Unit testing

- At the end of the work, we can validate all logical operations.

Radio Protocol Case itrust

Results and recommendations

Results

The results of the performance tests that we conducted showed that the LASP server can handle 100 users in the event that their requests are distributed over 10 seconds and the users send requests with a minimum interval of 10 seconds.

Recommendations

- Changing the way previous data used by some security checks is stored, or keeping old data in the memory to avoid requests to the database;
- Hosting the LASP service behind a fibre internet connection and setting a timeout after which the check will not be considered to compute the assurance level;
- Adapting the storage of data using threads to allow the application server to process normal computations without waiting for end of data storage.

Radio Protocol Case itrust

Exploitation

The LASP case study, conducted as part of the DIAMONDS project, allowed itrust to improve the LASP service and to help increase the performance and security of the service that will be delivered to the European Space Agency (ESA).

This not only provided good visibility for itrust, but also for the DIAMONDS project as a whole.