User requirements and Protection Profile for secure location sharing

EuroCAT 2010

24/08/2010

Julie Facon
Ben Fetler
Carlo Harpes
itrust consulting

itrust consulting s.à r.l.
Headquarter:
18, Steekaul
L-6831 Berbourg

Tel: +352 26 17 62 12
Fax: +352 26 710 378
Mail: Info@itrust.lu
Web: www.itrust.lu

Agenda

- Context and Privacy threats
- User requirements
- Security design with ISO 15408
- Outlook

Objectives

- Get familiar with security issues of Location-Based Service (LBS)
- Learn a methods for a (high-level) security design

Context

> Growing Location-Based Service

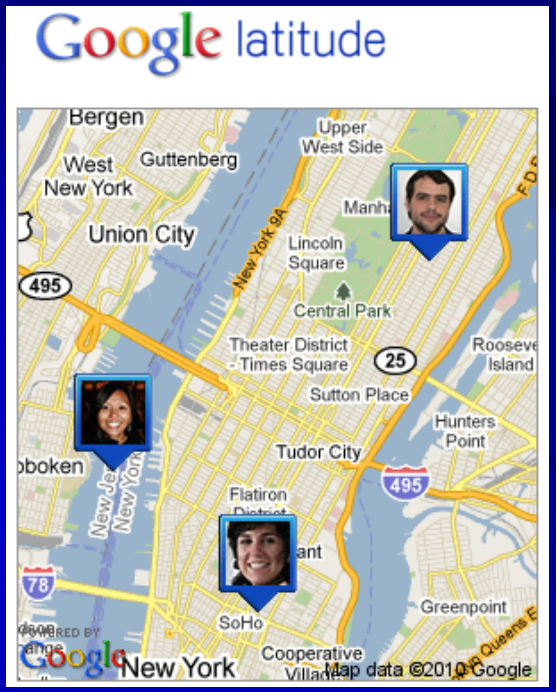
Many free services:

Geo-tagging

- on each iPhone, e.g.
- on Picture sites on the web

New service very easy to make

- built on free service Google Map and GeoAPI
- takes less than a week
- cf itrust-foetz.servehttp.com\Alidade

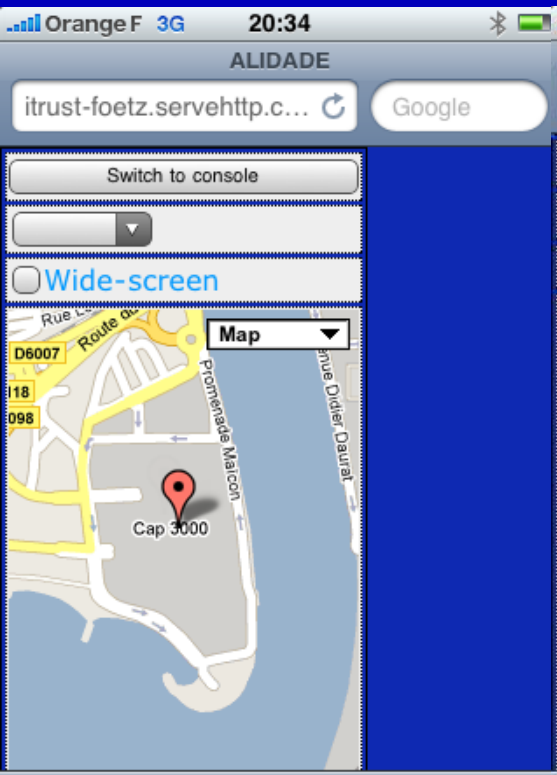


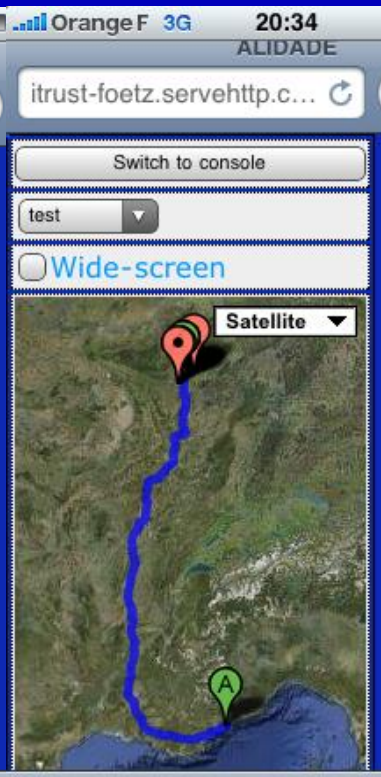
Context

> Growing Location-Based Service

New service very easy to make

- built on free service Google Map and GeoAPI
- takes less than a week
- cf itrust-foetz.servehttp.com\Alidade





itrust consulting s.à r.l.

Agenda

Context

> Little, but growing privacy awareness

No real care on passwords and shared information

- Social engineering for password very easy
- Very private info are shared with the entire world,
- cf www.cases.lu

Concerns by data privacy authorities

- Consumer organisation in Germany VZBZ asked users to quit Facebook
- Facebook asked to change form opt-out to opt-in before sharing personnel data
- EU data protection group faults Facebook for privacy setting change
- Google Buzz published list of followers without their consent, was criticised by several data protection authorities
- Opinion 5/2009 on online social networking (01189/09/EN WP 163): No search on location without explicit consent, access to near members is critisised.
- Cf www.cnpd.lu, ec.europa.eu

Context

> Questions

Is the user ready to pay for better privacy and security ?

How to build this security ?

How to get users trust in this security ?

Context

> Privacy options

Client-based versus network-based

- Client-based approach (e.g. GPS: the user computes his position) easier to secure than network-based approach (Apple: a service provider Skyhook tells you the location of the WiFi antenna you are currently using)
- The later provides possibility to trace users, abuse or sell data…
- Should we trust such service providers ?

Other publications

- Maya Gadzheva, Privacy concerns pertaining to location-based services, 2007.
- Jason Hong, etc , Privacy and Security in the Location-enhanced World Wide Web, 2003.
- Bill Schilit, etc , Wireless Location Privacy Protection, 2003.
- Agusti Solanas, etc , Location Privacy in Location-Based Services: Beyond TTP-based Schemes, 2008
- Louise Barkhuus, Privacy in Location-Based Services, Concerns vs. Coolness, 2004

User requirements

> Demo at Galileo Application Days (1/2)

Based on demo and questionnaires:

On March 2010, in Bruxelles
Not representative,
feedback from 32 questionnaires:

Functionalities:

People want to have a

- fast and easy to handle service
- with high accuracy (~1 meter (38%), ~10 meters (44%)),
- which could be installed on the most popular mobile phones.

Price:

OK for commercial service (73%),
with cost between 3 and 5 Euro per month (34%).

Target use is the family environment:

for localisation of their young children (40%) and of their elder family members (21%)

User requirements

> Demo at Galileo Application Days (2/2)

Main obstacle

- concern that data could be shared with other parties (39%),
- concern that they can get localised without their consent (31%)

Requirements:

- data to be stored securely
- operator be put under supervision of a Data Protection Authority (66%),

-> people have large concerns on their privacy.

Interpretation:

- in contradiction with the current popularity of unsecured social networks, and the willingness of peoples to share very private information.
- But it is consistent with the current public debates and the raised concerns on privacy issues.

Security design with ISO 15408

What is ISO 15408?

CC = Common Criteria

= an internationally standardised collection of criteria for the evaluation of security related products
http://www.commoncriteriaportal.org/

CC (ISO 15408) consists of three parts:

1. Introduction
2. Security Functional Requirements
3. Security Assurance Requirements
   (CEM = CC Evaluation Methodology
   = instructions for the evaluator how to verify the developer's compliance with the criteria)

Usage here

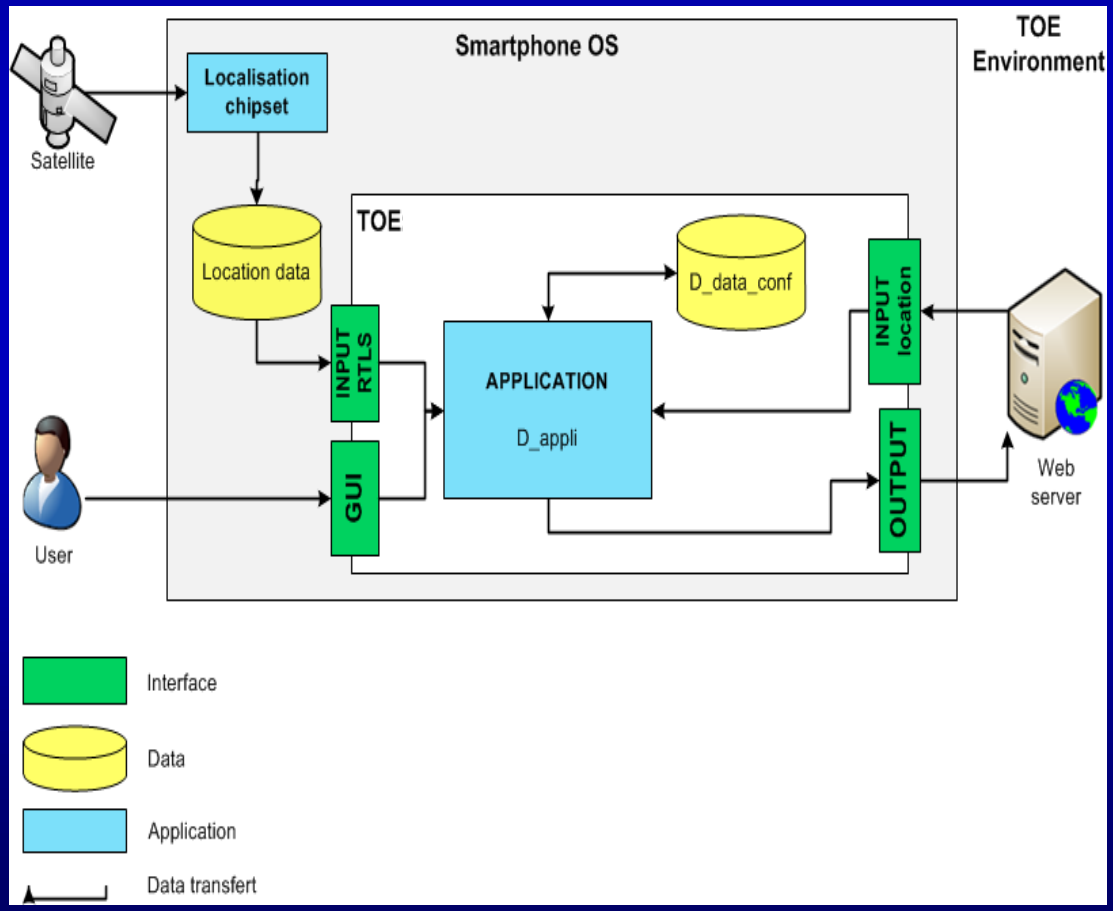
- Part 2 to design and document secure LBS in full transparency
- Later: certify that it is secure in the conditions that it has been designed for.

Security design with ISO 15408

What is ISO 15408?

Protection Profile

= security profile for a product called Target Of Evaluation



Security design with ISO 15408

TOE description

TOE type:

- Software software component for different devices such as Smartphone.
- Read location information of GPS chipset
- Send it regularly to a web server.
- Retrieve location of others from web server.

Usage:

- collect and send location data about people

Security objectives for operational environment

- The correct operation of the TOE depends on
  - the operating system on which it is installed,
  - on the hardware,
  - on the visibility of satellite signals, and
  - on the GSM network for external communication.

Security design with ISO 15408

Assets and threats

Assets:

D_Data: Location data which are transferred through the application from the GPS chipset to the web server.

D_Data_Conf: Configuration data of the application.

D_Application: The application which is installed on the smartphone.

Threats:

T_Confidentiality: Access to the location data by an unauthorized person or program by listening to the message or by accessing to configuration data through a second application. On data and config

T_Integrity: Modification of the application configuration. The application can be modified to send location data to a wrong server or to send wrong location data.
On data and config, not applic. as OS not under control

No availability as very hard to handle formally !

Security design with ISO 15408

Concerns for the design

Security objectives of the TOE :

- OT_Confidentiality: The location data has to be protected against access from unauthorized person.
- OT_Software_Integrity: The application should not be modified by a malware or an unauthorized person.
- OT_Data_Integrity: The data send by the software should not be manipulated before reception by the web server and vice versa.
- OT_Configuration_Integrity: The password should not be modified by an unauthorized person.

Security design with ISO 15408

Concerns for the operation

Assumptions:

A_User: The user is a person with honest intentions. He does not switch off the device or leave it at a wrong place.

Security objectives of the environment:

OE_Access: The Smartphone has to be protected by a password such as a SIM code or a password to open the application.

OE_Smartphone_Integrity: The Smartphone has to be protected against malware, virus and worms which can alter its process.

OE_Data_Integrity: The environment should verify that the location data has not been corrupted.

OE_Availability: Communication devices and networks which are used to transfer the location data by the application should be available.

Conclusion

And open questions

Findings

- It is easy to develop (unsecure) LBS.
- Users want security and require supervision of Service provider
- We recommend transparent security design and commitment to a protection profile.
- We defined a high-level model for general LBS security.
- Service provider should be prepared for certification.

Next steps:

- Implement, show compliance to protection profile (in a Security Target),
- Certify at recognised lab.
- Assure security of Web server by European Privacy Seal, hacking tests, etc.

Challenges:

- No control on global player (Google, Skyhook),
  - But they have a reputation to defend !
- No control on OS (Apple, e.g.)
- -> considerable limit on the final privacy

Questions & Discussion…

Thank you for your attention

Carlo Harpes

About itrust consulting

> Activities

(1) Management consulting

Risk Analysis:
- Value model
- Safeguard evaluation
- Risk map
- Risk status
- Deficiencies report

Computer Forensics

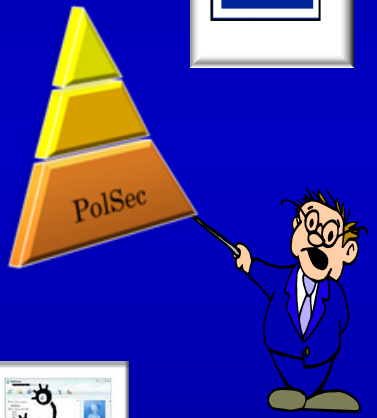
Audit

Crypto ← **Protocoles**

(2) Security consulting

Classification

SE	VIT	7 6
CO		5
RE	IMP	4
IN		3
PU	NOR	2 1



(3) Technical (and security) design

(4) Training and awareness

About itrust consulting

> Services

Consultancy

- ESA Studies LuxLAUNCH
- Security policies
- Information risk analysis

Audit

- Web Banking
- Proces certification
- Malware analysis
- ISO 27001,
- ISO 15408...

R&D – Technical and security design

- ESA: Secure Galileo localisation
- Incident manager
- Celtic, FP-7
- Risk Management Tool TRICK-Light

Multisourcing

- Security officer assistance
- SME security support (in preparation)

About itrust consulting

> Experiences of a research-making SME

itrust consulting s.à r.l.

Research in the strategy of itrust consulting

Acronym for
"**I**nformation : **T**echniques and
Research for **U**biquitous **S**ecurity and **T**rust"

Strategy:
from pure consulting to
mix between security design, support,
and consulting.

Past experience:
Essential support to sustainable growth in 2009:
6 employee with permanent contracts

Turnover 2009: 391k€

Tactic:
Maintain high rate of R&D in the next 3 years