Homeworks (and thesis) for the courses Sicurezza dei Sistemi Informatici (03GSD) and Computer Security (02KRQ) of the Politecnico di Torino academic year 2014-2015

Prof. Antonio Lioy
< lioy @ polito.it >

version 1.2 of 15/12/2015
Homework

- **max grade:**
  - 27 for the written part
  - 3 for the oral presentation (optional)

- **report:**
  - use Latex (see example at the web site)
  - about 30 pages
  - (optional) PPT slides for a brief talk (15-20’)

- **can be delivered at any time but – to record the grade in a certain session – MUST compulsory be delivered respecting the following deadlines:**
  - 20/2/2015 for recording the grade in February 2015
  - 26/6/2015 for recording the grade in July 2015
  - 11/9/2015 for recording the grade in September 2015
Homework outline

- meet your tutor to define your workplan
  - write down your workplan and send it to
    - your tutor and the teacher
    - for approval
- send periodic updates to the tutor and the teacher
  - brief (no more than 30 lines)
  - with clear reference to the workplan (items completed)
- it's possible to deliver ONE (at most TWO) draft version of the report to get feedback from the tutor/teacher:
  - assuming that the draft is delivered well in advance of the deadline for the final version
  - once the final report is delivered, it will be graded without any chance to further amend it
- please note that teacher and tutors are NOT available during August
Report skeleton

- introduction and state-of-the-art
- description of the new technique / analyzed solution
- advantages and disadvantages
- residual risks
- (when applicable) experimental performance analysis
- if the homework included the development or use of some programming code:
  - user manual (how-to for installation and use)
  - programmer manual (program logic, data and functions, how-to build)
- bibliography / sitography

**SHOULD DEMONSTRATE KNOWLEDGE OF COURSE’S TOPICS**
- … without useless repetitions
Picking up an homework

- contact the tutor to evaluate:
  - your real understanding of the subject
  - pre-requisites

- homeworks already assigned are marked with one or more X in the title (one X per person, up to the maximum number of people allowed for the homework)
Note about homeworks with several students

- the role of each student must be clear (to get individual evaluation)
- at the same time, it must be clear the benefit of having done a joint homework (i.e. some common part such as a common introduction or a joint experiment)
Homework and graduation work (thesis)

- your homework may be the first part of your final graduation work (a.k.a. thesis)
- if you want to do your thesis in the computer security area then let the teacher know this before getting the homework
- in this case do NOT select a specific homework but select a thesis project and contact the teacher for getting a suitable subject inside the project
- thesis subjects related to EU research projects often have a possible direct connection with:
  - a stage or job at one of the project's partners (as well as at POLITO)
  - pursuing a PhD title
Final notes

- look for updates of this document (e.g. subjects already assigned, addition of new subjects)
  - each version is identified as X.Y (major.minor)
  - the major number is changed when new subjects are added
  - the minor number is changed when a subject is assigned to a student

- if you are interested in computer security but can’t find a suitable subject in this list (are you kidding me?) then you can propose your own subject
Elenco dei progetti di ricerca per tesi

/  

Possible research projects for thesis
Research projects (I)

- SECURED project (www.secured-fp7.eu)
  - medium (3 M Euro) EU project for offloading security from user terminals to a secure and trusted network element at the edge of the network
  - partners: POLITO, Telefonica, HP, PrimeTel, UNICRI, UPC, VTT
  - possible subjects:
    - security policies (specification, management and translation)
    - ontologies and automatic reasoning
    - automatic network and system configuration of security parameters
    - security optimization
    - trusted network connections
    - trusted execution environment (based on virtual machines)
    - remote attestation
  - requirements:
    - C or Java programming
  - environment:
    - Linux (preferred) or Windows
  - contact: LIOY or BASILE / cataldo.basile@polito.it
Trusted Computing, i.e. what is my trust foundation?

- in my network are there only my computers?
- my computers are running only the sw selected by me?
- is the sw configured in the proper way?
- when I use a public network (e.g. Internet) rather than a private network, am I really connected to the expected node?
- when I am connected to a server, how can I verify its application sw is the “good” one or it has been altered?

answers: Trusted Computing (and Trusted Network Connection)

- TPM for desktop, MTM for mobile (or equivalent solutions)
- TC-enhanced Linux + trusted virtualization
- remote attestation & TLS
Components of a TC system

- **local / remote attestation**
  - proof of configuration (whole sw stack)

- **isolation**
  - execution in separate domains / compartments / environments

- **protected memory**
  - hw key container
  - data encryption
  - data sealing

- **secure I/O**
  - towards the user
  - among various components
Research projects (II)

- **ASPIRE project** (http://www.aspire-fp7.eu/)
  - partners: U. Gent, Gemalto, Nagravision, POLITO, Safenet, U. East London,
  - contact: BASILE (cataldo.basile@polito.it / 7173)

- **topic**
  - advanced software protection

- **project objective**
  - improve software protection with new advanced and stronger techniques
  - precisely measure the reached level of protection
  - target mobile platforms

- **features**
  - work on a challenging research topic
    - ASPIRE looks for solution against powerful Man-at-the-End attackers
  - face with real problems from market leading companies
    - abstract research topics are leveraged by real problems from world leading companies having high security requirements
ASPIRE subjects

- research objectives
  - remote software attestation
  - software optimization
  - empirical analysis of software protection
- remote attestation
  - develop a framework to add remote attestation functionality to an existing program
  - investigate new criteria for attesting software
- formal model of software attacks and protection
  - models to understand how to protect a software given the assets given attacks and software protection dependencies
- optimization of software protection
  - given the formal model, define optimization programs to select which is the best way to protect a software
- …and we invite you to participate to contests to empirically evaluate the strength of developed software protections
ASPIRE Consortium

Fondazione Bruno Kessler
Universiteit Gent
Politecnico di Torino
University of East London
Gemalto
Nagra
Kudelski Group
SafeNet
Research projects (III)

- STORK 2.0 project (www.eid-stork2.eu)
  - large (58 partners, ~10 M Euro) EU project for interoperability of e-ID
  - possible subjects:
    - digital identity (SAML, XACML, id federation)
    - public-key certificates, digital signatures, PKI
    - e-ID implementation (smart-card, smartphones, NFC, …)
    - e-government applications
  - requirements:
    - Java programming
    - web programming
  - environment:
    - Linux (preferred) or Windows
- contact: LIOY or BERCARU / diana.berbecaru@polito.it
Research projects (IV)

- **CLIPS project**
  - European project started on February 2014
  - security of cloud computing
  - possible subjects:
    - risk analysis of specific architectures
    - integration of Stork e-ID with cloud management systems
    - remote attestation and secure log of activities
  - requirements:
    - C or Java programming
  - environment:
    - Linux
**Research projects (V)**

- **TENACE project**
  - Italian project started in 2013
  - trusted and secure environment for protection of critical infrastructures (CI)
  - possible subjects:
    - security model of CI
    - security policy for a CI
    - automatic analysis / simulation of a CI
  - requirements:
    - C or Java programming
  - environment:
    - Linux
Elenco delle tesine / tesi proposte
(in aggiunta alle tesi sui progetti di ricerca)

Possible homeworks and thesis
(in addition to the thesis subjects associated to the research projects)
Cloud attestation (homework/thesis)

- **tutor:**
  - LIOY / lioy@polito.it / 011 0907021
  - SMIRAGLIA / paolo.smiraglia@polito.it / 011 0907192

- **topic:**
  - how to apply trusted computing attestation to a cloud environment
  - for application to SECURED (https://www.secured-fp7.eu/)

- **people:** up to 3

- **example references:**
  - scientific literature on the topic

- **outline:**
  - (homework) state-of-the-art in this field
  - (thesis) state-of-the-art in this field + design of a (partial) solution + implementation

- **required skills (for thesis):** Java or C++, Linux (basic sysadmin knowledge)
**SDN security (homework/thesis) = XX-**

- **tutor:**
  - LIOY / lioy@polito.it / 011 0907021
  - RISSO / fulvio.risso@polito.it / 011 0907008

- **topic:**
  - software-defined networking (SDN) is a new network paradigm to implement custom network paths over a common fabric, by decoupling the control and data planes (http://en.wikipedia.org/wiki/Software-defined_networking)
  - however its security (if any) is highly questionable and we want to investigate this topic for application to SECURED (https://www.secured-fp7.eu/)

- **people: up to 3**
  - (homework) Treccarichi + Pulvirenti

- **example references:**
  - scientific literature on the topic (e.g. http://dx.doi.org/10.1109/SDN4FNS.2013.6702553)

- **outline:**
  - (homework) state-of-the-art in this field
  - (thesis) state-of-the-art in this field + design of a (partial) solution + implementation

- **required skills (for thesis):** Java or C++, Linux (basic sysadmin knowledge)
Network Functions Virtualisation (NFV) is a new network paradigm to implement network functions as virtual elements available on commodity hardware distributed inside a network and then orchestrated. ETSI is leading its definition (www.etsi.org/technologies-clusters/technologies/nfv) however its security is still an open issue and we want to investigate this topic for application to SECURED (https://www.secured-fp7.eu/).
SECURED: policy workflow

1. **User connects to policy editor**
   - HSPL specification
   - MSPL specification

2. **Policy refinement**
   - MSPL (user)

3. **Policy analysis**
   - Policy reconciliation
   - Policy translation
   - MSPL (reconciled)
   - Low level

4. **User connects to the NED**
   - MSPL (ISP3)
   - MSPL (corporate)
   - User policy stack layers
   - MSPL policies

Note: T4.1, T4.2, T4.3, T4.4, and outside are likely part of the diagram's color-coding or categorization system.
SECURED: policy system architecture

Data layer

- policy stack (user level)
- policy stack (infrastructure level)
- MSPL
- HSPL
- user PSA info
- PSA Manifest
- M2L plugin
- actual configuration settings

Translator (M2L) Plugin

User reports

- REPORT SCA
- REPORT MCA
- REPORT REC
- REPORT REF+N-ENF
- REPORT EN-ENF

User interface

Policy stack (user level)
Policy stack (infrastructure level)
MSPL
HSPL
User PSA info
PSA Manifest
M2L plugin
Translator Service (M2L)
Actual configuration settings

API interfaces

Single user Conflict Analysis
Multiple user Conflict Analysis
Reconciliation
Refinement
Early Non-enforceability

Manifest

Translator (M2L) Plugin

User reports

REPORT SCA
REPORT MCA
REPORT REC
REPORT REF+N-ENF
REPORT EN-ENF

User interface

Policy stack (user level)
Policy stack (infrastructure level)
MSPL
HSPL
User PSA info
PSA Manifest
M2L plugin
Translator Service (M2L)
Actual configuration settings

API interfaces

Single user Conflict Analysis
Multiple user Conflict Analysis
Reconciliation
Refinement
Early Non-enforceability

Manifest

Translator (M2L) Plugin

User reports

REPORT SCA
REPORT MCA
REPORT REC
REPORT REF+N-ENF
REPORT EN-ENF

User interface
Secured: policy translation and policy support tools

- **policy translation: from MSPL to actual configurations (M2L)**
  - to transform an abstract policy (described in MSPL) into the configuration format used by a specific PSA

- **Security Policy Management (SPM) service architecture**
  - **Policy Editor**
    - a web-based management system for end-users to define their policies, create profiles for quick enforcement (and sharing)
    - HSPL
    - MSPL
  - **Policy Report**
    - a web-based management system for end-users to their user policies report
  - **Policy Manager**
    - manages all the policy-related workflows
  - **Access Control Unit**
    - manages authorization to all the policy objects and PSAs
Translator plug-in for IPsec (homework)

- tutor:
  - VALLINI / marco.vallini@polito.it / 011 0907192
  - VALENZA / fulvio.valenza@polito.it / 011 0907192

- topic:
  - automatic generation of an IPsec configuration starting from security models

- people: 1

- example references:
  - Openswan (https://www.openswan.org/) or FreeS/WAN (http://www.freeswan.org/)
  - SECURED (https://www.secured-fp7.eu/)

- outline:
  - analysis of security model to represent channel protection
  - analysis of IPsec (security properties, features, etc)
  - analysis of Openswan or FreeS/WAN configuration settings
  - development of a plug-in to translate channel protection into Openswan or FreeS/WAN configuration settings

- required skills: Java, Linux (basic sysadmin knowledge)
Policy definition support system (homework/thesis)

- tutor:
  - VALLINI / marco.vallini@polito.it / 011 0907192
  - VALENZA / fulvio.valenza@polito.it / 011 0907192
- topic:
  - assisted high-level policy definition
- people: 1
- example references:
  - documents on policy grammar
  - SECURED (https://www.secured-fp7.eu/)
- outline:
  - analysis of high-level policy models
  - analysis of decision support system techniques for policy processing
  - development of software module to define and edit policies
- required skills: Java, Linux (basic sysadmin knowledge)
Policy conflict analysis report (thesis)

- tutor:
  - PITSCHIEIDER / christian.pitscheider@polito.it / 011 0907192
  - VALENZA / fulvio.valenza@polito.it / 011 0907192

- topic:
  - automatic generation of policy conflicts report

- people: 1

- example references:
  - SECURED (https://www.secured-fp7.eu/)

- outline:
  - analysis of conflict types
  - define a novel approach to represent conflicts
  - development of a software module to generate a HTML report

- required skills: Java, HTML/JS
Policy reconciliation report (thesis)

- tutor:
  - PITSCHEIDER / christian.pitscheider@polito.it / 011 0907192
  - VALENZA / fulvio.valenza@polito.it / 011 0907192

- topic:
  - automatic generation of policy reconciliation report

- people: 1

- example references:
  - SECURED (https://www.secured-fp7.eu/)

- outline:
  - analysis of reconciliation strategies
  - define a novel approach to represent reconciliation strategies
  - development of a software module to generate an HTML report

- required skills: Java, HTML/JS
Simulation of security in a network (thesis)

- tutor:
  - VALLINI / marco.vallini@polito.it / 011 0907192
  - VALENZA / fulvio.valenza@polito.it / 011 0907192
  - PITSCHIEDER / christian.pitscheider@polito.it / 011 0907192

- topic:
  - validation of security configuration by using simulation tools

- people: 1

- example references:
  - Mininet (http://mininet.org/)
  - OpenFlow (https://www.opennetworking.org/sdn-resources/onf-specifications/openflow)

- outline:
  - analysis of OpenFlow protocol
  - analysis of security configuration and enforcement
  - analysis of simulation tools (e.g. mininet)
  - development of validation strategies and configuration assessment

- required skills: Java, Linux (basic sysadmin knowledge)
Analysis of IPsec implementations (homework) = X

- tutor: ATZENI / shocked@polito.it / 7173
- topic:
  - this homework aim is to evaluate and compare the readily available implementation tool for IPsec (namely strongSwan, freeSwan, Racoon, ...) from a number of points of view
- people: 1
  - Vincenzo Costanzo
- example references:
  - http://www.strongswan.org
- outline:
  - analysis of
    - functional modes
    - configuration
    - RFC implemented
    - comparison
Distributed security attacks analysis (homework - XX)

- tutor: ATZENI / shocked@polito.it / 7173
- topic:
  - distributed attacks (e.g. DDoS, large scale spam) are used in last years by organised crime and national-scale entities. From a technical point of view, what are the details of last years “successful” threats?
- people: 1-2
  - Giovanni Iovino e Rocco Santomo
- example references:
- outline:
  - technical analysis of last year distributed attacks
  - definition of a taxonomy/properties for the analyzed attacks
Mobile OSs analysis (homework - XX)

- tutor: ATZENI / shocked@polito.it / 7173
- topic
  - analysis and comparison of the security model of recently released mobile “operating systems"
- people: 1-2
  - Alessio Canepa e Andrea Marcelli
- co-work with Telecom Italia Lab
- example reference:
  - Ubuntu Touch, Firefox OS, Tizen, WebOS, …
- project (details to be agreed with the tutor and Telecom Italia Lab researchers):
  - theoretical analysis of the mobile OS platform
  - practical testing on physical HW
IT security cost estimation (thesis)

- tutor: ATZENI / shocked@polito.it / 7173
- topic
  - estimation of security costs is presently a point open to debate. What are the current solutions? How much are they suitable in practice?
- people: 1
- reference:
  - www.gao.gov/assets/600/592273.pdf
- project:
  - review of the scientific state of the art (rules, tools, standards)
  - development of scenarios and use cases to apply different standards analysed
  - development of a tool based on the state of the art review
Software security testing (thesis)

- **tutor**: ATZENI / shocked@polito.it / 7173
- **topic**: automatic testing to assess security properties (like confidentiality and integrity), is a complex task. This thesis plans to improve the state of the art by automating specific steps and developing usable solution for developed software.
- **people**: 1
- **example references**:
  - http://dx.doi.org/10.1016/S0164-1212(97)00167-2

- **project (details to be agreed with the tutor)**:
  - state of the art review
  - identification of weaknesses
  - design of automatable steps
  - development of working prototype
Cloud based risk-management tool (thesis)

- tutor: ATZENI / shocked@polito.it / 7173
- topic
  - during last decade, many risk-analysis (RA) methodologies have been developed. Since the large-scale adoption of cloud-based solutions, should be desirable update risk-analysis flow, in the light of changes introduced by this paradigm
- people: 1
- references:
  - example of tools available in risk-analysis (e.g. Pilar: http://www.ar-tools.com/en/index.html) and vulnerability assessment and mitigation (e.g. nexpose http://www.rapid7.com/products/nexpose/ ) tools
- project (details to be agreed with the tutor):
  - analyse available RA methodologies and computer aiding tools to identify weaknesses in respect of cloud-based assessment.
  - identify weak points (in respect of cloud-based solutions)
  - design improvements
  - implement selected improvements
Secure coding (thesis)

- **tutor**: ATZENI / shocked@polito.it / 7173
- **topic**
  - mobile and convergent software development (e.g. based on javascript) lacks of specifically tuned secure coding methodologies. The development of security bug-free code, is required to avoid presence of disconcerting security flaws. This thesis wants to investigate state of the art, and then improve the state of the art proposing and testing a methodology for secure code development

- **people**: 1
- **references**:
  - selected documents (papers + project internal documents)
- **project (details to be agreed with the tutor)**:
  - analysis of available methodologies for automated code check and application to selected environment
  - development of best-practices shaped for mobile secure coding,
  - experiment of secure coding methodology
  - application to selected tools-open source projects
Usable security (thesis)

- tutor: ATZENI / shocked@polito.it / 7173
- topic
  - often, security is developed not devoting proper care to usability. Since the user base is largely composed by unaware security people, this aspect have to be refined, mixing up concepts from different disciplines (e.g. cognitive science, user friendliness) to enrich the security model.
- people: 1-2
- possible co-work with Bournemouth University
- example references:
  - http://www.computer.org/portal/web/csdl doi/10.1109/ARES.2011.115
- project (details to be agreed with the tutor):
  - critical analysis of present security models, with respect to usability
  - development and refinement of the present usability models, with respect to tangible results like privacy preserving interfaces
  - design and development of selected prototypes
  - assessment of results with practical experiments (e.g. focus groups)
Security engineering IDS (thesis)

- Tutor: ATZENI / shocked@polito.it / 7173
- Topic
  - IDS can work at host or/and at network level. A level still not addressed, from an automatic point of view, is the human level, in spite of the fact that human beings are still the weakest link in the security chain. This thesis would analyze human behaviour related to security threats, in order to develop a novel IDS/IPS capable to detect and possibly react to on-going malicious physical actions.
- People: 1-2
- Possible co-work with Bournemouth University
- Reference:
  - Selected document to be discussed with the tutor
- Project
  - Review of the scientific state of the art (rules, tools, standards best practices)
  - Design of system and human model (particular reference to persona)
  - Prototype implementation
Thesis: SSG – Security Serious Games

- Tutor: ATZENI / shocked@polito.it / 7173
- Topic:
  - Serious games are a recent tendency to exploit games for specific training. Even if some serious game has been developed in the field of security (e.g. Computer Forensics) the security field has still not been addressed. Purpose of the thesis is to apply serious game methodology for developing a proof of concept security serious game.
- People: 1-2
- Co-work with Bournemouth University
- Reference:
  - Selected document to be discussed with the tutor
- Project:
  - Review of the scientific state of the art (rules, tools, standards best practices)
  - Design of the game requirements (goals, user models)
  - Development of the proof of concept
RAISE - Risk Analysis Integration with Security Engineering (thesis)

- **tutor:** ATZENI / shocked@polito.it / 7173

- **topic**
  - Risk analysis is a required task to drive rational security choices at enterprise level. Some risk analysis steps have been made automatic, while other are very difficult to manage automatically. This thesis aims to investigate possible methodologies to model social engineering part, in order to be integrated in semi-automated risk analysis tools.

- **people:** 1-2

- **possible co-work with Bournemouth University**

- **reference:**
  - selected document to be discussed with the tutor

- **project**
  - Review of the scientific state of the art (rules, modelling tools)
  - Applicability of concepts (e.g. personas)
  - Development and integration in risk analysis workflow
Hpfeed analysis and evolution (thesis)

- tutor: ATZENI / shocked@polito.it / 7173
- topic
  - Hpfeed is a protocol largely used in Honeynet project. As part of previous thesis the protocol has been implemented in C++ for the sake of security and performance. Next step is to study and possibly improve the protocol from both specification and implementation points of view.
- people: 1
- example reference:
  - https://redmine.honeynet.org/projects/hpfeeds/wiki
- possible co-work with Telecom Italia Lab
- project (details to be agreed with the tutor and Telecom Italia Lab researchers):
  - analysis of the state-of-the-art for lightweight authenticated publish/subscribe protocol
  - modelling and formal analysis of the C++ implementation
  - alternative message-exchange protocol design and implementation
**SDR jammer (thesis)**

- **tutor:** ATZENI / shocked@polito.it / 7173
- **topic**
  - SDR (Software Defined Radio) allows to develop and program “home-made” jammer without use of too much costly hardware. The thesis aims to develop USRP jammers for GSM and UMTS terminals, using the Telecom Italia Lab test-bed and hardware.
- **people:** 1
- **possible co-work with Telecom Italia Lab**
- **project (details to be agreed with the tutor and Telecom Italia Lab researchers):**
  - analysis of the background (jammer, GSM and UMTS protocols, SDR, ...)
  - state of the art of 2G, 3G and 4G jamming
  - analysis of the available software libraries
  - development of suitable scenarios / use cases
  - development, configuration, testing (using Telecom Italia Test Plant) of SDR's jammer
Controlled Android box (thesis)

- tutor: ATZENI / shocked@polito.it / 7173
- topic:
  - evolution of an Android-based system (initially designed and developed in a previous thesis work) to control the smartphone usage in specific scenarios (e.g. parental control for children)
- people: 1
- possible co-work with CSP
- example references:
  - previous thesis report
- project (details to be agreed with the tutor):
  - analysis of the state-of-the-art
  - critical analysis of the present framework and implementation
  - enrichment of present framework
  - testing of the developed tool
Remote Attestation in STORK (homework)

- tutors:
  - SMIRAGLIA / paolo.smiraglia@polito.it / 7192
  - BARRESI / nicola.barresi@polito.it / 7192

- topic:
  - integration of Remote Attestation techniques in STORK-based authentication.

- people: 1

- example references:
  - https://www.eid-stork.eu
  - https://01.org/openattestation

- outline:
  - overview about federated authentication models (STORK, OpenID, …)
  - overview about Trusted Computing (TCG) and Remote Attestation (OpenAttestation)
  - scenario and integration plan definition
  - proof of concept implementation

- required skills: Java, Linux (sysadmin knowledge)
STORK authentication in Keystone (homework)

- **tutors:**
  - SMIRAGLIA / paolo.smiraglia@polito.it / 7192
  - BARRESI / nicola.barresi@polito.it / 7192

- **topic:**
  - add support for STORK authentication to OpenStack’s identity manager (Keystone).

- **people:** 1

- **example references:**
  - https://www.eid-stork.eu
  - http://docs.openstack.org/developer/keystone/

- **outline:**
  - overview about centralized and federated authentication models
  - overview about STORK-based authentication
  - extension of Keystone API for supporting STORK-based authentication

- **required skills:** Python, Linux (sysadmin knowledge)
Logging in the cloud (homework)

- **tutor:**
  - SMIRAGLIA / paolo.smiraglia@polito.it / 7192

- **topic:**
  - state of the art about Cloud-oriented logging frameworks.

- **people:** 1-2

- **example references:**
  - http://www.fluentd.org
  - http://flume.apache.org
  - http://www.graylog2.org/

- **outline:**
  - state of the art about logging in a Cloud
  - analysis and test of software for remote logging management

- **required skills:** Linux (advanced sysadmin knowledge)
VANET tools (thesis)

- **tutor:** BASILE/cataldo.basile@polito.it /7173
  - with Panos Panadimitratos from KTH Stockholm
- **topic:**
  - VANET (Vehicular Ad hoc NETwork) is an emerging standard. It may offer new services to drivers, on the other hand it may create privacy issues
  - a privacy solution has been proposed using pseudonyms
- **people:** 1-2
- **references:**
  - selected documents (papers + project internal documents)
- **project (details to be agreed with the tutor):**
  - (1) testing the threat model
  - (2) provide new Apps (services) based on location (accident reconstruction, highway code violations)