GDPR and legal challenges for designing distance bounding protocols

Mirosław Kutyłowski

Politechnika Wrocławska

Cryptacus Training School, Ponta Delgada 2018

Security in system design

- security of all parties involved must be concerned, not only of a user
- ... in particular security of the system designer
- many things may go wrong:
  - financial claims against system designer based on system errors
  - pressure from the authorities on system designer to misbehave
  - pressure on certificate/audit bodies to provide false evidence
  - mistakes during implementation
  - patent claims
  - ...

Security and privacy

Standard approaches to ensure Security and Privacy

- criminal law
- certification/audit frameworks
- industrial standards
- legal contracts

Criminal law

Situation in EU

- in most countries the same roots of the legal system (Roman Empire)
- there are two incompatible systems: continental law, common law
- the same ideas occur in European countries, however practically there are deep differences based on details
- even more differences with USA

German criminal law versus system design

Section 202a, Data espionage

1. Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.
2. Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.

German criminal law versus system design

Section 202b, Phishing

Whosoever unlawfully intercepts data (section 202a(2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment not exceeding two years or a fine, unless the offense incurs a more severe penalty under other provisions.

German criminal law versus system design

Section 202c Acts preparatory to data espionage and phishing

1. Whosoever prepares the commission of an offense under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible
   1. passwords or other security codes enabling access to data (section 202a(2)), or
   2. software for the purpose of the commission of such an offense,

   shall be liable to imprisonment not exceeding one year or a fine.

German criminal law versus system design

Section 203 Violation of private secrets

(1) Whosoever unlawfully discloses a secret of another, in particular, a secret which belongs to the sphere of personal privacy or a business or trade secret, which was confided to or otherwise made known to him in his capacity as a ... [here a narrow closed list] ...

German criminal law versus system design

Section 204, Exploitation of the secrets of another

(1) Whosoever unlawfully exploits the secret of another, in particular a business or trade secret, which he is obliged to keep secret pursuant to section 203, shall be liable to imprisonment not exceeding two years or a fine.

German criminal law versus system design

Section 206 Violation of the postal and telecommunications secret

1. Whosoever unlawfully discloses to another person facts which are subject to the postal or telecommunications secret and which became known to him as the owner or employee of an enterprise in the business of providing postal or telecommunications services, shall be liable to ...
2. Whosoever, as an owner or employee of an enterprise indicated in subsection (1) above unlawfully
   1. opens a piece of sealed mail ...

   shall incur the same penalty.

German criminal law versus system design

Section 263a, Computer fraud

1. Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing shall be liable to imprisonment not exceeding five years or a fine.
2. The attempt shall be punishable.

German criminal law versus system design

Section 263a, Computer fraud

3. In especially serious cases the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender
   1. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of forgery or fraud;
   2. causes a major financial loss of or acts with the intent of placing a large number of persons in danger of financial loss by the continued commission of offenses of fraud;
   3. places another person in financial hardship;
   4. abuses his powers or his position as a public official ; or

Common Criteria

Common Criteria Framework

Goals

1. a common evaluation framework
2. guide for a customer to choose the right product

However

1. **CC certificate is not a security guarantee**
2. it is frequently misunderstood as a security certificate
3. processing cost is still high

Common Criteria Framework

Idea

1. write a Protection Profile based on evaluation of risks (PP)
2. build a product according to Protection Profile (Security Target, ST)
3. audit the product according to a very formalized procedure by a certification body

- ease the process,
- reuse work,
- build from standard components

Common Criteria Framework

CC certificate contribution

- CC certification says that a product has been developed according to a given PP (or ST)
- assurance level concerns only the stated requirements, e.g. trivial requirements $\Rightarrow$high EAL level (possible mistake: demanding high EAL level without specifying PP)

Protection Profile

Target of Evaluation (TOE)

“is aimed at potential consumers who are looking through lists of evaluated TOEs/Products to find TOEs that may meet their security needs, and are supported by their hardware, software and firmware”

Protection Profile

important sections of TOE

- Usage and major security features of the TOE
  - crucial properties of the system (high level) and security features from the point of view of the security effect and not how it is achieved
- life-cycle
  - the product in the whole life cycle including manufacturing, delivery and destroying
- TOE type
  - which parts, which general purpose, which functionalities are present and which are missing, e.g. ATM card with no contactless payments
- Required non-TOE hardware/software/firmware
  - other components that can be crucial for evaluation

Protection Profile

Conformance Claim

- CC Conformance Claim: version of CC
- PP claim: other PP taken into account in a plug-and-play way
- Package claim: which EAL package level

Protection Profile

EAL

- 6 “assurance classes”
- subdivided into 27 sub-categories (the so-called “assurance families”)
- for each assurance family – grading of an evaluation: a number
- EAL result: an array of 27 values
- 7 predefined ratings, called evaluation assurance levels or EALs. called EAL1 to EAL7, with EAL1 the lowest and EAL7 the highest
- e.g.: EAL2 assigns the rating 2 to 7 assurance families, the rating 1 to 11 assurance families, and 0 to the other 9 assurance families
- monotonic: EALn+1 gives at least the same assurance level as EALn in each assurance family

Example assurance family
ALC_FLR Flaw remediation

ALC_FLR.1

- The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
- The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
- The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
- The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

Example assurance family
ALC_FLR Flaw remediation

ALC_FLR.2:

- ALC_FLR.1 as before
- The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
- The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.
- The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
- The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Protection Profile

Security Problem Definition

OSP Object Security Problem : "The security problem definition defines the security problem that is to be addressed."

axiomatic : deriving the security problem definition outside the scope of CC

crucial: "the usefulness of the results of an evaluation strongly depends on the security problem definition"

requires work : "spend significant resources and use well-defined processes and analyses to derive a good security problem definition"

Protection Profile
Security Problem Definition

assets

entities that someone places value upon.
E.g. contents of a file, - distance correctness, - presence at a given place, - anonymity with respect to an external observer

threats

threats to assets, what may happen that would endanger an asset

assets versus threats

- a mapping matrix: mark which threat endangers which asset
- an asset which is not the subject of any threat can be disregarded
- from this point we are not talking about assets but only threats

Protection Profile

Security objectives

The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition.

Role of SO

- a high-level, natural language solution of the problem;
- divide this solution into part-wise solutions, each addressing a part of the problem;
- demonstrate that these part-wise solutions form a complete solution to the problem.
- bridge between the security problem and Security Functional Requirements (SFR)

Example of SO: *the token communicates only with legitimate readers*

Protection Profile
SO

mapping

- mapping objectives to threats: a matrix with SO and threats
  each threat should be covered, each objective has to respond to some threat
- answers the question:
  - what is sufficient to avoid threats?
  - have we forgot about something?
- rationale: a verifiable explanation why the mapping is sound

after this stage we may forget about threats and think about SOs only

Protection Profile

SFR (Security Functional requirements)

- SFRs are a translation of the security objectives for the TOE.
- a complete translation (the security objectives must be completely addressed)
- SFRs should be independent of any specific technical solution (implementation)
- standardized language - to ease evaluation and comparison

Protection Profile

SFRs catalogue

- many SFRs already predefined via CC
- possibility to add own ones
- customizing possible in most cases (options left for the writer of a PP)

Protection Profile

examples of predefined classes

- Logging and audit class FAU
- Identification and authentication class FIA
- Cryptographic operation class FCS
- Access control families FDP_ACC, FDP_ACF
- Information flow control families FDP_IFC, FDP_IF
- Management functions class FMT
- (Technical) protection of user data families FDP_RIP, FDP_ITT, FDP_ROL
- (Technical) protection of TSF data class FPT
- ...

Common Criteria
summary

- "compose from pieces" approach (versus monolithic approach)
- checkable: divide-and-conquer approach
- key security issue: poorly written PP $\Rightarrow$ insecure system

Standards

Standards versus security

- standardization is a process of getting a compromise regarding choice of technical details,
- security relevant consequences:
  - it is better to have one target to analyze/attack than potentially unlimited number of choices
  - compromise is almost always not driven by security issues
  - not a transparent process, security specialists might be missing in the team

Threat: many decision makers regard a technical standard as a security guarantee.

Contracts

Typical practices

no responsibility for correct operation, “use program as it is”

theoretically a user can try to negotiate better conditions, but it is nearly impossible

GDPR changes the situation dramatically – with regard to personal data protection

Privacy protection and GDPR

Privacy by design

GDPR

1. General Data Protection Regulation in EU
2. scope:
   - activities in EU
   - exporting such data
   - activities outside Europe concerning commercial services in EU
3. in practice enforcing the same regime elsewhere

"devices compliant with GDPR"

GDPR

Technical scope

GDPR "applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."

most systems processing data in systematic way fulfill these conditions

GDPR

personal data

any information relating to an identified or identifiable natural person (“data subject”);

an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

recommendation

whenever possible create systems so that data cannot be linked to a natural person

GDPR

processing

any operation or set of operations

which is performed on personal data or on sets of personal data,

whether or not by automated means,

such as collection, recording, organization, structuring, storage,adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

corollary

possessing personal data already means “processing”. destroying is also processing and must be lawful

GDPR

pseudonymisation

processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

corollary

pseudonymisation reversible with additional keys

apply whenever it might be necessary to recover the link to a natural person

GDPR
actors

controller ... body which determines the purposes and means of the processing of personal data;

processor ... processes personal data on behalf of the controller;

GDPR
rules of processing

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject
"lawfulness, fairness and transparency";

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, ... not be considered to be incompatible with the initial purposes
"purpose limitation";

GDPR
rules of processing

Personal data shall be:

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed "data minimization"

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay "accuracy"

GDPR
rules of processing

Personal data shall be:

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ... "storage limitation"

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures "integrity and confidentiality"

GDPR
privacy by design

accountability

The controller shall be responsible for, and **be able to demonstrate compliance** with [these rules]

- **provable security!**
- not regarding an abstract model but **reality**
- the previous regulation referred to responsibility only

GDPR lawful processing

Conditions for lawful processing

1. the data subject has given consent to the processing ... for one or more specific purposes;
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject ...

GDPR

Conditions for consent

1. ... the controller shall be able to demonstrate that the data subject has consented to processing ...
2. The data subject shall have the right to withdraw his or her consent at any time.
3. ... It shall be as easy to withdraw as to give consent.

extra requirements for enabling to leave the system and remove data

GDPR

Problems with biometric data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, ... shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies: ...

corollary

avoid any processing of biometric data,
if you must process biometric data, then particular care during system design is necessary

GDPR

Information to the data subject

The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

consequences

- automatic processing necessary
- completeness of information
- centralized information retrieval

GDPR

who gets the data

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(e) the recipients or categories of recipients of the personal data, if any;

GDPR

Information obligations

In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

- ...

consequence

the controller must have an information channel to the data subject

GDPR

Right of access by the data subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;

- ...

consequences

- online access for a user?
- you have to be particularly careful about transfering data outside Europe

GDPR
right-to-be-forgotten

The data subject shall have the right to obtain from the controller the erasure of personal data ... without undue delay ... where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes ...

(b) the data subject withdraws consent on which the processing is based according to and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds ...

(d) the personal data have been unlawfully processed;

...

consequences

- problems for distributed ledgers
- automated (erasure) processing versus examination of legal situation

GDPR
further topics

1. right for correcting information
2. profiling users and the right to object
3. data portability

Security obligations of the controller and the processor

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,

   the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

   (a) the pseudonymisation and encryption of personal data;
   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

GDPR

Security obligations of the controller and the processor

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

GDPR
penalties

Administrative fines for controllers and processors

up to 20.000.000 EUR up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher

depending on the art of the problem

the upper bounds established so that they are not negligible for big players from USA, but for small enterprises ....

Identification challenge

identification

- in most scenarios if two devices interact, then they have to present their identifiers
- but if they communicate over an open channel
- .. there is no privacy-by-design

asymmetric crypto

- establish a secure channel - e.g. with Diffie-Hellman
- exchange identity data over secure channel

symmetric crypto

???

tracing threats might be hard to avoid for lightweight devices, a significant challenge to implement systems according to GDPR