# *Quality Attributes and Associated Tactics for Privacy-by-Design*

Antonio Kung

August 21st, 2013

## Quality Attributes for Privacy-by-Design

[Bass03] defines a quality attribute (QA) as a *measurable or testable property of a system that is used to indicate how well the system satisfies the needs of its stakeholders*. There can be many QAs. For instance [Bass03] covers the following: availability, interoperability, modifiability, performance, security, testability, usability.

The impact of privacy-by-design on engineering has been addressed by [Spiekermann09, Gürses11, Kung11]. Based on this material, we have identified the following QAs for privacy-by-design:

* *Minimization*. Minimization measures the level of data processing limitation. [Gürses11] points out that minimization is the foundational principle for privacy-by-design.
* *Data protection*. It measures how well the system is protected against privacy leaks (accidental or malicious), i.e. against data processing events that do not conform to the specified collection, use, disclosure and retention limit. Data protection can be viewed as a security quality attribute.
* *Accountability*. Accountability measures how well the system can identify misconducts leading to privacy leaks. This quality attribute leads to more transparency, one of the pillars for privacy-by-design identified in [Kung11].
* *Modifiability*. Modifiability measures the ease of system change.

## Tactics for Privacy-by-Design

### Minimization Tactics

Minimization tactics measures the level of data processing limitation. Here are two minimization tactics:

* *Anonymize credentials*. This tactic allows users to prove statements about themselves anonymously, for instance the user can prove that he is over 18 without revealing his birthdate. It is based on cryptographic techniques such as zero-knowledge proofs. Direct anonymous attestation is another example of technique which enables the remote authentication of a trusted platform whilst preserving the user's privacy.
* *Limit processing perimeter*. This tactic is used in distributed systems to reduce the perimeter where processing and storage takes place. For instance limiting processing at the client level guarantees that user personal data is processed and kept in its personal device (smart phone, home device, vehicle device).

### Data Protection Tactics

Data protection tactics measures the security of data processing. Here are two data protection tactics:

* *Enforce data processing policies*. This tactic is used to verify that only allowed data collection, data access and usage, and data retention operations are performed. Techniques for enforcing policies include access control, automatic data removal, encryption of data, firewalls and so forth.
* *Protect processing*. This tactic is used to protect the system against accidental or malicious operations that may lead to data leaks. Examples of techniques are data storage protection (e.g. Hippocratic database), communication protection (e.g. authenticity and confidentiality), processing protection (e.g. Security processor, virtualization through hypervisors).

### Accountability Tactics

Accountability measures how well the system can identify misconducts leading to privacy leaks. Here are three accountability tactics:

* *Log data transaction*. This tactic allows users to examine what operations were carried out concerning their personal data.
* *Log modifications*. This tactic allows stakeholders to examine what modifications were made to improve the system conformance to privacy (policies, crypto, protection).
* *Protect log data*. This tactic is used to ensure that log data cannot be changed. For instance TPM[[1]](#footnote-1) can be used to securely sign such data.

### Modifiability Tactics

Modifiability measures the ease of system change. Here are three modifiability tactics:

* *Change policy*. This tactic allows for the modification of policy in order to improve data protection
* *Change crypto strength and method*. This tactic allows for the modification of a crypto strength (e.g. longer keys) and method (e.g. new cryptographic protocol) in order to improve data protection
* *Change protection strength*. This tactic allows for the modification of the processing protection (e.g. switching from a standard database to a Hippocratic data base)..

## References

[Agrawal02] R.Agrawal, J.Kiernan, R.Srikant, Y.Xu. “Hippocratic Databases”, 28th International Conference on Very Large Data Bases, Hong Kong, August 2002

[Bass03] L.Bass, P.Clements, R.Kazman. “Software Architecture in Practice”, 3rd Edition, Addison-Wesley, 2012.

[Gürses11] S. F. Gürses, C. Troncoso, and C. Diaz. “Engineering Privacy-by-Design”. Computers, Privacy & Data Protection, January 2011

[Kung11] A.Kung, J.Freytag, F.Kargl. “Privacy-by-design in ITS applications”. 2nd IEEE International Workshop on Data Security and Privacy in wireless Networks, June 20, 2011, Lucca, Italy

[Spiekermann09] S.Spiekermann, L.Cranor. “Privacy Engineering”. IEEE Transactions on Software Engineering, Vol. 35, Nr. 1, January/February 2009, pp. 67-82

1. See <http://www.trustedcomputinggroup.org/> [↑](#footnote-ref-1)