Messung von Aspekten der Vertrauenswürdigkeit in der Softwareentwicklung

Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

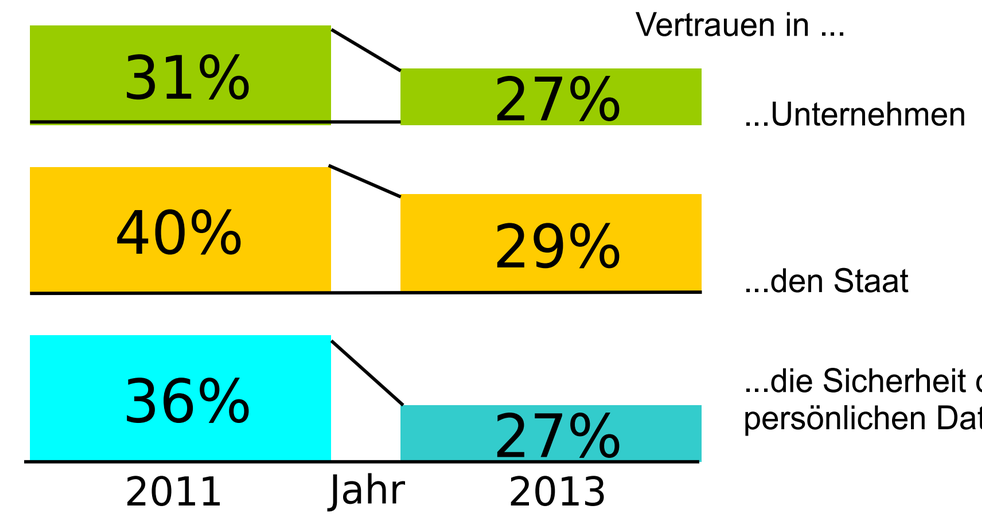
Sandro Hartenstein, M. Sc.
sandro.h@rtenstein.com
metrictool.eu 25.1.2016

Einleitung

Die **Vertrauenswürdigkeit** von Software wird primär durch Sicherheits- und Qualitätseigenschaften definiert. Grundlage zur Bewertung von **Softwaresicherheit** ist die Identifikation von Schwachstellen. Das bekannteste Evaluierungsframework *Common Criteria* und der von Microsoft veröffentlichte Prozess *Microsoft Secure Development Lifecycle* setzen auf diese Schwachstellen- und Risikoanalysen.[1,2]
Im Bereich der **Softwarequalität** liegt der Fokus auf den nicht-funktionalen Eigenschaften. Für diese können Referenzwerte zur Bewertung der Qualität ermittelt werden.[3]
Die konstruktive **Messung** und Bewertung von **nicht-funktionalen Eigenschaften** wurde auf den ganzheitlichen Kontext der **Vertrauenswürdigkeit** von Software übertragen. Daraus ergibt sich die Forschungsfrage:

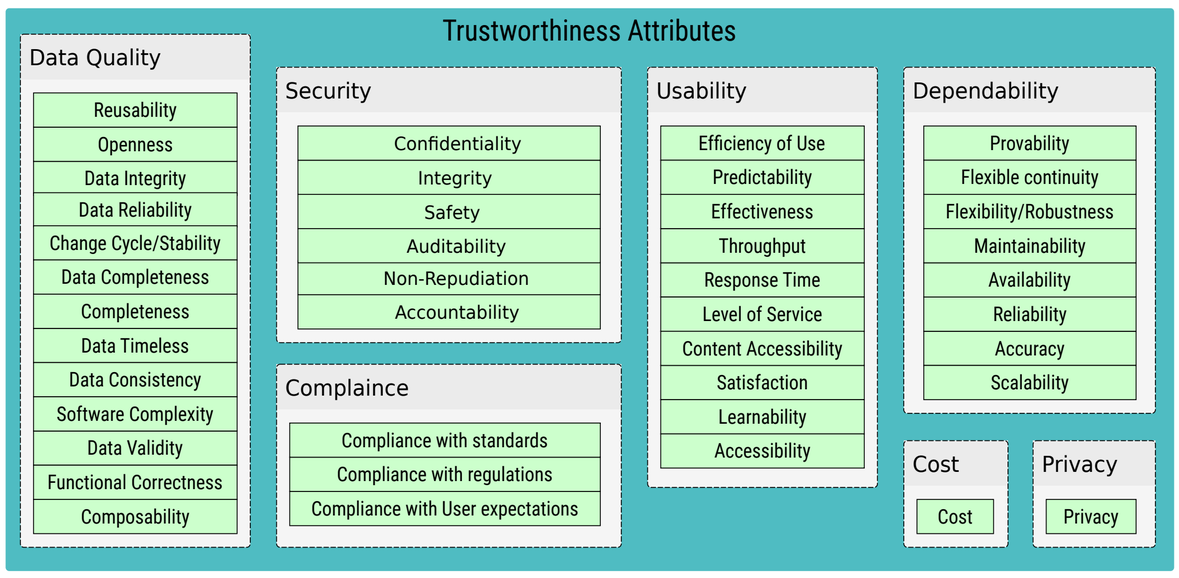
Inwieweit erlaubt die Anwendung von Software-Metriken entlang des Entwicklungsprozesses eine wirksame und effiziente Steuerung der Vertrauenswürdigkeit von Software?

Problemstellung



Das Vertrauen der Anwender in Unternehmen, Staat und in die Sicherheit der persönlichen Daten ist nach einer Umfrage des Branchenverbandes Bitkom in den Jahren 2011 bis 2013 sichtbar gesunken.[4]
Besonders die Messung der **Vertrauenswürdigkeit** von Software der neuen Anwendungsgebieten (Internet of Things, BigData, SmartCities und Industrie 4.0) bietet den **Anwendern** die Möglichkeit, Systeme eigenständig zu bewerten und so **Vertrauen aufzubauen**.

Forschungsstand

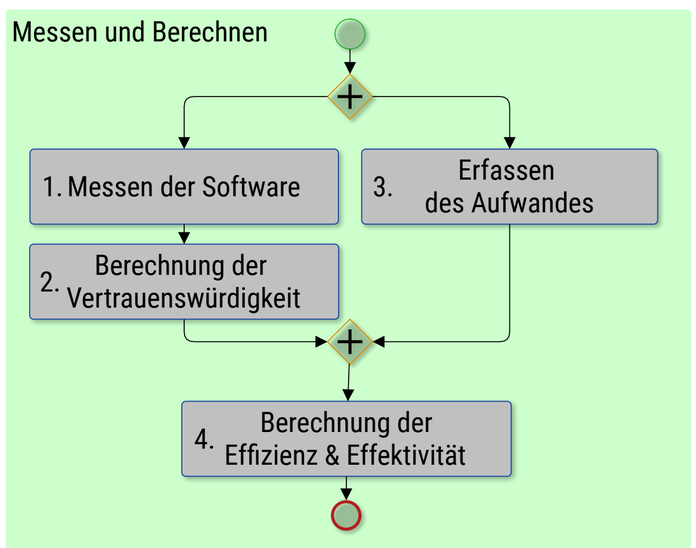


Zur Bestimmung der **Vertrauenswürdigkeit** werden 42 **Attribute** verwendet (Abb. rechts).[5]
Diese Attribute sind mit Hilfe von 134 **Metriken** quantifizierbar (Bsp. in Abb. unten). Es werden die Betrachtungskontexte **Entwicklung**, **Marktplatz** und **Laufzeit** addressiert.[6]

metric id: APP-ENG-Storeencr-01

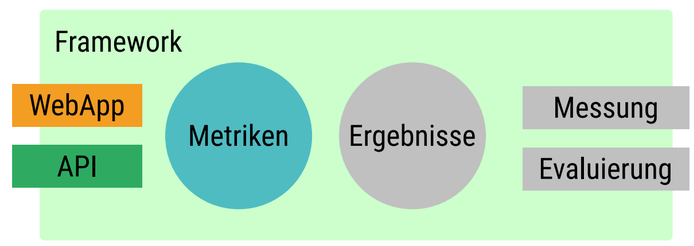
name: stored encrypted data	composition type: avarage	status: final
formula: X = A / B * 100%	context: engineering	attribute: confidentiality
description: The percentage of the stored encrypted data is determined.		
computation: x = (∑ encrypted user objects / ∑ user objects) *100%		

Methode



1. Messung von Parametern über den Entwicklungszyklus der Software
2. Berechnung, Speicherung der Vertrauenswürdigkeit (Nutzen)
3. Erfassung des Aufwandes für die Messung der Vertrauenswürdigkeit
4. Berechnung der Effizienz (Wirtschaftlichkeit = Nutzen / Aufwand) und Berechnung der Effektivität (Wirksamkeit = Nutzen / Ziel (100%))

Status



Das Mess- und Berechnungsframework ist zu 50% fertiggestellt. Im Anschluss ist die Untersuchung und Auswertung konkreter Software geplant.

Literatur

1. CCRA: Common Methodology for Information Technology Security Evaluation Evaluation methodology September 2012 Revision 4 Foreword: Common Methodology for Information Technology Security Evaluation Evaluation methodology September 2012 Revision 4 Foreword. 2012.URL http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R4.pdf
2. Microsoft: Security Development Lifecycle. URL http://www.microsoft.com/security/sdl/default.aspx – Überprüfungsdatum 2014-11-22
3. Khan, Khaled M.: Software Security Engineering. In: International Journal of Secure Software Engineering 3 (2012), Nr. 1, S. 62–63
4. Prof Dieter Kempf: Sicherheit und Vertrauen im Netz: Sicherheit und Vertrauen im Netz. Berlin : 25.7.2013. URL http://www.bitkom.org/files/documents/BITKOM_PK_Sicherheit_im_Netz_Charts_25_07_2013.pdf
5. Paulus, Sachar ; Mohammadi, Nazila Gol ; Weyer, Thorsten: Trustworthy Software Development, Bd. 8099. In: Hutchison, David; Kanade, Takeo; Kittler, Josef; Kleinberg, Jon M.; Mattern, Friedemann; Mitchell, John C.; Naor, Moni; Nierstrasz, Oscar; Pandu Rangan, C.; Steffen, Bernhard; Sudan, Madhu; Terzopoulos, Demetri; Tygar, Doug; Vardi, Moshe Y.; Weikum, Gerhard; Decker, Bart de; Dittmann, Jana; Kraetzer, Christian; Vielhauer, Claus (Hrsg.): Communications and Multimedia Security. Berlin, Heidelberg : Springer Berlin Heidelberg, 2013 (Lecture Notes in Computer Science), S. 233–247
6. Hartenstein, Sandro ; Könnecke, Holger ; Paulus, Sachar: TRUSTWORTHINESS METRICS FOR SOCIO-TECHNICAL SOFTWARE. In: Thoma, Klaus (Hrsg.): 9th future security : Berlin, September 16 - 18, 2014 ; proceedings. Stuttgart : Fraunhofer-Verl, 2014, S. 673–682