Toolunterstütztes Messen der Vertrauenswürdigkeit von Webapplikationen

Sandro Hartenstein (M.Sc.)

OPTET Operational Trustworthiness Enabling Technologies

Fachhochschule Brandenburg University of Applied Sciences

Zusammenfassung:
Diese Forschungsarbeit entstand an der FH Brandenburg im Rahmen des EU-FP7 Projektes **operational trustworthiness enabling technologies**, kurz OPTET. Die Entwicklung von Methoden und Tools zur Optimierung der Vertrauenswürdigkeit von Webapplikationen sind die Ziele des Projektes. Das Team der FH Brandenburg hat die Messung der Vertrauenswürdigkeit mit Hilfe von Metriken als Aufgabe. Diese Präsentation zeigt die Motivation, die Methoden und die wichtigsten Ergebnisse. Ideen für weitere Forschung und Entwicklung werden im Ausblick dargestellt.

Ausgangspunkt

Die **Vertrauenswürdigkeit** von Software wird primär durch **Sicherheit- und Qualitätseigenschaften** definiert.

Grundlage zur Bewertung von **Softwaresicherheit** ist die identifikation von Schwachstellen.

Das bekannteste Evaluierung-Framework *Common Criteria* und der von Microsoft veröffentlichte Prozess *Microsoft Secure Development Lifecycle* setzen auf diese Schwachstellen- und Risikoanalysen.[1,2]

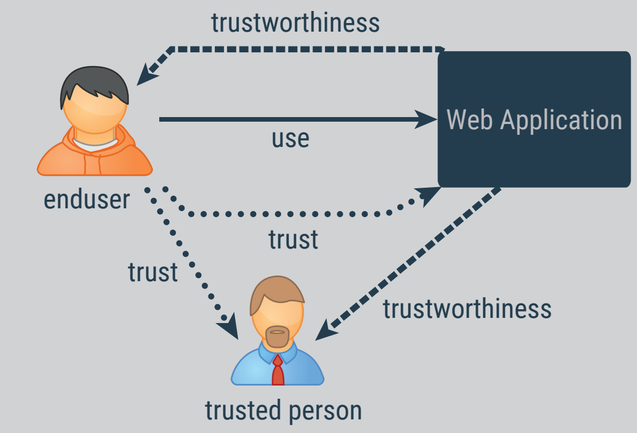
Im Bereich der **Softwarequalität** liegt der Fokus auf den nicht-funktionalen Eigenschaften. Für diese können Referenzwerte zur Bewertung der Qualität ermittelt werden.[3]

In diesem Forschungsvorhaben wird die konstruktive Messung und Bewertung von nicht-funktionalen Eigenschaften auf den ganzheitlichen Kontext der Vertrauenswürdigkeit von Software übertragen.

Die Schwachstellen werden dabei nicht direkt gemessen und bewertet, sondern fließen in die neu definierten Messziele ein.

Grundlage und Motivation

Vertrauen vs. Vertrauenswürdigkeit

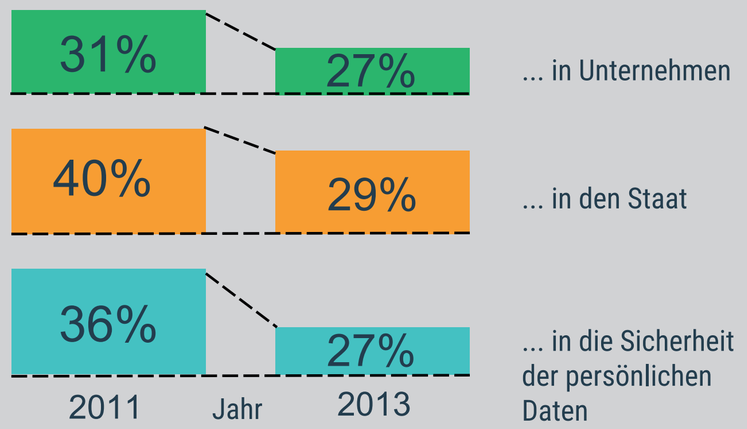


Die Entscheidung eines Anwenders für oder gegen eine Anwendung basiert auf den Einflussfaktoren **Vertrauen** und **Vertrauenswürdigkeit**.

Als **objektive Eigenschaft** der Anwendung ist die **Vertrauenswürdigkeit** messbar und von der Entwicklung der Software charakterisiert.

Im Unterschied dazu ist das **Vertrauen** eine individuelle **subjektive Wahrnehmung** der Software vom Standpunkt des Anwenders.[4]

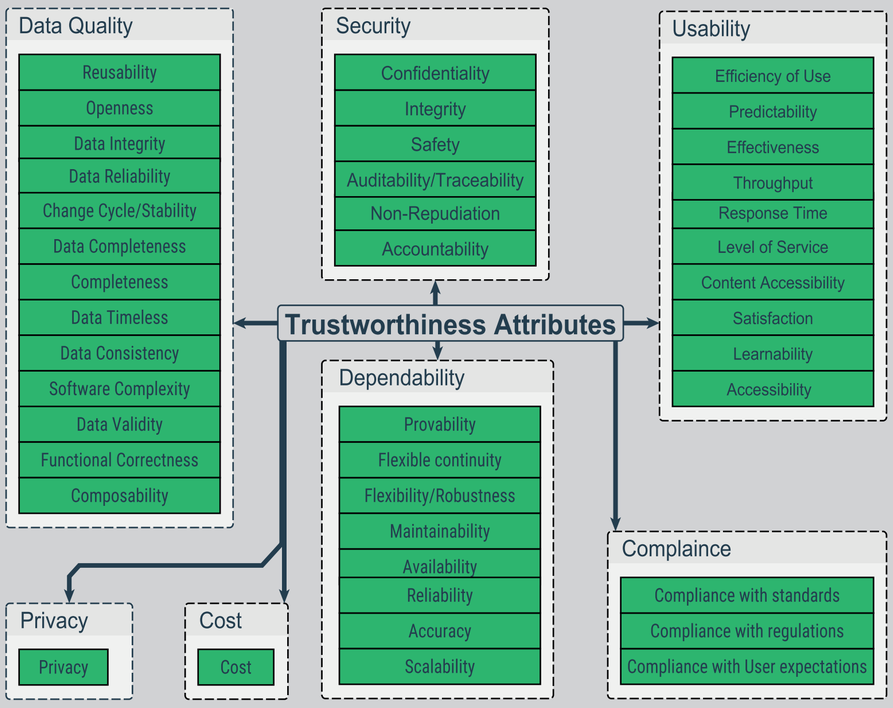
Sinkendes Vertrauen



Das **Vertrauen** der Anwender in Unternehmen, Staat und in die Sicherheit der persönlichen Daten ist in den Jahren 2011 bis 2013 **sichtbar gesunken**.[5]

Die Messung der Vertrauenswürdigkeit unterstützt den Anwender bei der Bewertung von Software. Daraus ergibt sich die Chance, **Vertrauen** in Technologien **zurück zu gewinnen**.

Methode



Schritt 1: Attribute der Vertrauenswürdigkeit

Zur Bestimmung der Vertrauenswürdigkeit wurden **42 Attribute** ermittelt. Grundlage ist die Analyse der wichtigsten Standards, Normen und Best Practices aus den Bereichen Sicherheit und Qualität.[6]

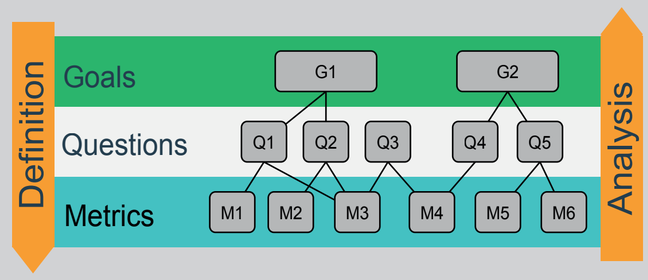
Schritt 2: Metriken mit Goal Question Metrics

Mithilfe der Goal Question Metrics Methode nach Victor Basili wurden Metriken entwickelt.[7]

In der **Definitionsphase** wird für jedes Attribut ein Ziel definiert. Die benötigten Messpunkte und Messobjekte werden durch Fragen ermittelt. Die Antworten auf die jeweiligen Fragen sind Metriken.

In der **Analysephase** werden die Metriken mit den Parametern des Untersuchungsobjektes berechnet, Fragen beantwortet und den Grad der Erreichung des Ziels festgestellt.

Die entwickelten Metriken unterscheiden sich im **Betrachtungskontext**. Untersucht wurden **Entwicklung**, **Marktplatz** und **Laufzeit**. In der Entwicklungsphase ist der Quelltext einer Anwendung durchsuchbar, im Marktplatzkontext steht nur die fertige Anwendung zur Verfügung und zur Laufzeit ist die Software im Einsatz.



Ergebnis

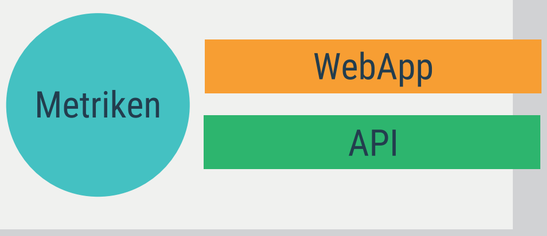
Metriken

Das Ergebnis sind 134 Produktmetriken.[8]

In der Tabelle ist beispielhaft eine Metrik aus dem Entwicklungskontext für das Attribute Vertraulichkeit aufgeführt.

Metrik	APP-ENG-Storeencr-01
name	stored encrypted data
attribute	confidentiality
context	engineering
description	The percentage of the stored encrypted data is determined.
metric	Percentage user objects that support encryption
metric_computation	x = (sum of user objects that support encryption / sum of user objects) *100%
formula	X = A / B * 100
GQM : goal	The data that is considered confidential used must be kept confidential at any time and at any place.
GQM : question	How much % of the data that is considered confidential is stored in encrypted form?

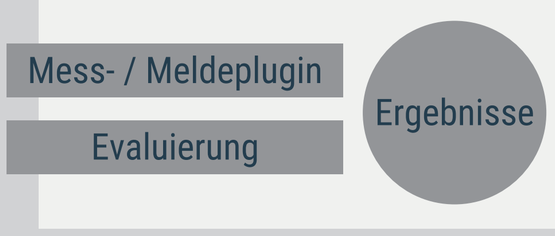
Software



Die Bereitstellung der Metriken erfolgt durch ein **Metrictool**. Es besteht aus einer **Webapplikation** und einer **Berechnungsapi**. Über die Weboberfläche können die Metriken und deren Zusatzinformationen verwaltet werden. Die Schnittstelle ermöglicht die Berechnung von Metriken und stellt Zusatzinformationen bereit.

Ausblick

Erweiterung



Die toolunterstützte Messung der Vertrauenswürdigkeit von Software kann durch Erweiterung des Metrictools verbessert werden.

Im Bereich der Messung ist ein Plugin zur **Codeanalyse und Rückmeldung** an den Programmierer in Planung.
Die Auswertung wird mit Unterstützung einer **Speicherung der Ergebnisse** beabsichtigt. Die Veränderung der Vertrauenswürdigkeit im Verlauf der Entwicklung einer Software kann so sichtbar gemacht werden. Diese Daten können auch verwendet werden, um die Metriken zu evaluieren.
Eine **Effektivitäts- und Effizienzanalyse** der Messung von Vertrauenswürdigkeit auf Basis von den Daten, welche mit Hilfe des Frameworks gewonnen werden, wird angestrebt.

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. IT Innovation ; AUEB ; IMinds ; FHB: Socio - economic requirements for trust and trustworthiness. URL http://www.optet.eu/wp-content/uploads/2013/09/OPTET_WP2_D2.1_SocioEconomic_Requirements_V1.1.pdf
5. 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
6. 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
7. Basili, V.R., G. Caldiera, H.D. Rombach (1994): Goal Question Metric Paradigm. In Marciniak (ed.), Encyclopedia of Software Engineering, John Wiley & Sons, 528-532. http://www.cs.umd.edu/~basili/publications/technical/T87.pdf
8. 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

Sandro Hartenstein (M.Sc.)
sandro.h@rtenstein.com
metrictool.eu | optet.eu | fh-brandenburg.de

03.11.2015

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 317631 (OPTET)