Das KIARA Security-Modell

Andreas Nonnengart · Dmitri Rubinstein
Philipp Slusallek · Werner Stephan

Deutsches Forschungszentrum für
Künstliche Intelligenz – DFKI GmbH
{nonnengart | rubinstein | slusallek | stephan}@dfki.de

Zusammenfassung

In den letzten Jahren ist zunehmend die Tendenz zu erkennen, das Design von komplexen Anlagen aus einer kompositionalen und somit nicht-monolithischen Perspektive zu betrachten. Gleiches gilt seit jüngerer Zeit für die IT-Sicherheit. In diesem Papier stellen wir das KIARA-Sicherheitsmodell vor, wie es im Rahmen des FIWARE-Programms der EU entworfen und implementiert wurde. Im obigen Sinne agiert KIARA lokal auf den Knoten eines Netzwerks und nicht auf einer zentralisierten Sicherheitskomponente. Globale Sicherheitseigenschaften ergeben sich aus dem über feste Regeln definierten Zusammenspiel der einzelnen lokalen Sicherheitsbedürfnisse und Garantien.

1 Einleitung

Bei KIARA handelt es sich um einen neuartigen Middleware-Ansatz, der im Rahmen des großen Future Internet Programms der EU (FI-PPP) entwickelt und realisiert wird, [FIW]. Hauptanliegen ist die Bereitstellung von Verfahren zur hoch-effizienten und -sicheren Kommunikation zwischen Software-Komponenten, die über verschiedene Hard- und Software-Plattformen verteilt und über eine Vielzahl von Kommunikationsmechanismen miteinander verbunden sind.

In Bezug auf die IT-Sicherheit war eine so genannte „eingebaute Sicherheit (Security by Design)“ zentraler Leitgedanke bei der Entwicklung der verschiedenen, neuartigen Sicherheitskonzepte von KIARA. Im Gegensatz zu heute verbreiteten Ansätzen, [Blak00, OMG14], in denen „Schutzwälle“ auf Netzwerkebene eine Absicherung realisieren sollen, wird hier die Verantwortlichkeit und die damit verbundene „Intelligenz“ in KIARA auf die Knoten des Netzwerks übertragen, siehe Abbildung 1. Wesentliche Motivation dabei war, dass eine klare Trennung zwischen guter Innenwelt und bedrohlicher Außenwelt nicht mehr möglich ist. Heutige Entwicklungen im Bereich Industrie 4.0, Cloud Computing und dem Internet der Dinge verlangen nach flexiblen, dynamisch konfigurierbaren und dezentral organisierten Schutzmechanismen. Anstelle der Aufweichung eines starren Schutzwallprinzips durch immer neue Sonderregelungen werden Kommunikationsbeziehungen zwischen Netzwerkkomponenten feingranular strukturiert, wie in Abschnitt 2 beschrieben. Dies bietet dann die Möglichkeit, wechselseitig diesen Strukturen zugeordnete Forderungen und Garantien abzugleichen.

Diese beziehen sich auf eine Vielzahl von sicherheitsrelevanten, anwendungspezifischen Aspekten. Zur Beherrschung der Komplexität und Änderungsfreundlichkeit trägt dabei eine streng lokale Sicht bei: Jede Komponente verfolgt einerseits eigene Sicherheitsinteressen durch For-

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 168-176.

derungen an Kommunikationspartner und bietet anderseits bestimmte Garantien für diese. Entscheidungen bezüglich eingehender Daten und ausgehender Daten gründen dabei nicht einfach nur auf einem abstrakten Begriff des Vertrauens (beispielsweise ausgedrückt durch Zertifikate), sondern einer Beschreibung von Sicherheitseigenschaften, die bestimmten, einzelnen Strukturen zugeordnet sind.

Bei Verhandlungen werden die jeweils von der anderen Seite gelieferte Garantien, beschrieben in einer konfigurierbaren Zusicherungssprache, analysiert, indem deklarativ beschriebene Sicherheitspolitiken in der Middleware ausgeführt werden. Mögliche eigene Garantien sind mit dieser Politik auf Grundlage eines semantischen Modells verknüpft. Die grundlegende Vorgehensweise wird in Abschnitt 3 beschrieben.

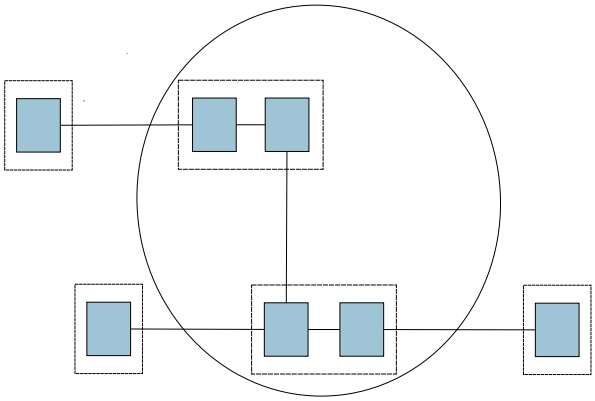

Abb. 1: Schutzwall zur Trennung von Innen und Außen

Wie in Abschnitt 4 diskutiert, kann das korrekte Zusammenwirken der lokalen Politiken und Garantien auf der deklarativen Ebene überprüft werden (in einigen Fällen sogar auf mechanische Weise), mit dem Ziel sinnvolle, semantisch untermauerte globale Eigenschaften zu garantieren. Diese Eigenschaften sind im Rahmen eines geeigneten Informationsflussbegriffs formal ausdrückbar.

Um höhere Vertrauenswürdigkeitsstufen zu erreichen, müssen die von der KIARA-Middleware angebotenen Sicherheitsdienste um zusätzliche Maßnahmen, siehe Abschnitt 5, ergänzt werden. Dazu gehören die Separierung und Einkapselung von Applikationen und der Aufbau sicherer Kanäle.

KIARA wurde nicht nur im Sinne einer eingebauten Sicherheit konzipiert, sondern unterstützt auch kompositionale Bewertungsprozesse. Diese Aspekte werden im Abschnitt 6 diskutiert.

2 KIARA Netzwerke

Wie oben bereits erwähnt, bezieht sich die Sicherheit in KIARA auf ganze *Netzwerke* von *Knoten*. Die *Knoten* eines KIARA-Netzwerks bestehen aus Applikationen, die über die KIARA-Middleware kommunizieren.

Schon für komplexe einzelne Plattformen hat sich schon bald nach dem Aufkommen der ersten Sicherheitspolitiken gezeigt, dass monolithische Lösungen unrealistisch sind. Um zu einer

geregelten Koexistenz von Einheiten (Bereichen) mit unterschiedlichen (Sicherheits-) Anforderungen und Vertrauenswürdigkeitsstufen zu kommen, bedarf es

- technischer Maßnahmen zum Schutz vor einer unkontrollierten Beeinflussung und
- konzeptueller Lösungen für die Interaktion von Knoten mit jeweils lokalen Sicherheitspolitiken.

Der erste Punkt wird in Abschnitt 5 aufgegriffen. Der Abgleich von Forderungen und Garantien, die sich aus lokalen Sicherheitspolitiken ergeben, ist zentraler Bestandteil des KIARA Ansatzes. Forderungen und Garantien beziehen sich auf Kommunikationsobjekte von Schnittstellen, durch die der Informationsaustausch strukturiert wird. Dabei gibt es Objekte für eingehende ($\bigcirc$) und ausgehende ($\square$) Informationen.

Im *Client-Server*-Ansatz, der gegenwärtig implementiert ist, bestehen Schnittstellen auf Seiten eines Clients a aus Funktionsdeklarationen der Form $\tau_r^i \leftarrow f^i(\tau_0^i, \ldots, \tau_{n-1}^i)$. Auf der Serverseite b gibt es in der Anwendung eine möglicherweise passende Realisierung $\tau_r^j \leftarrow f^j(\tau_0^i, \ldots, \tau_{n-1}^j)$. Wenn ein solcher Match $i \mapsto j$ aus Sicht der beteiligten Datentypen τ realisiert werden kann, findet eine wechselseitige Sicherheitsverhandlung statt, welche auf den Anforderungen der einen Seite und den Garantien der jeweils anderen Seite beruht. Diese entscheidet darüber, ob $< i, j >$ Teil einer (möglicherweise schon bestehenden) Verbindung $< a, c, b >$ sein kann.

Im Allgemeinen kann jeder Knoten sowohl als Client wie auch als Server agieren; für eine bestehende Verbindung $< a, c, b >$ betrachten wir aber den Knoten a als den Client und den Knoten b als den Server.

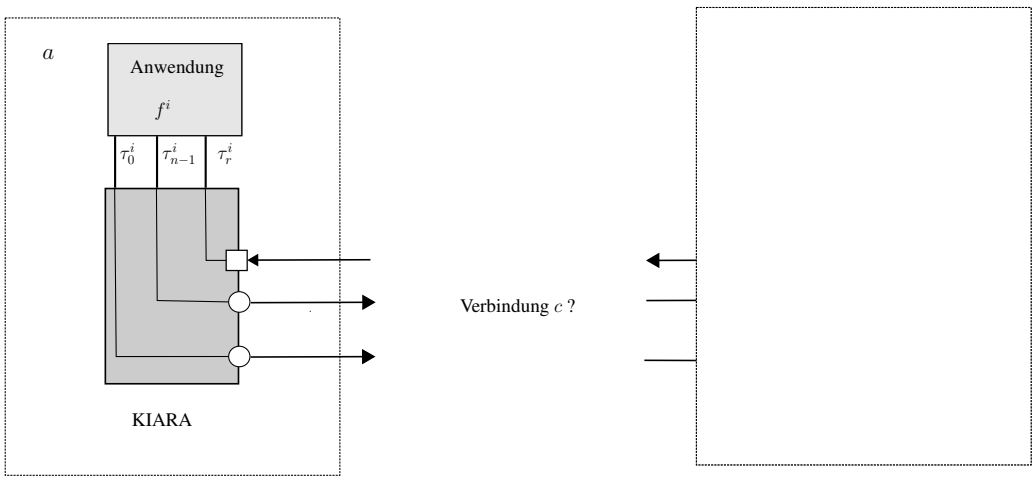

Abb. 2: Knoten in einem KIARA-Netzwerk

Während der teilweise dynamisch erzeugte Programmcode, der den tatsächlichen Transport der Daten in KIARA realisiert, die Umwandlung von Datentypen mit beinhaltet, beziehen sich Sicherheits-Annotationen – wie unten beschrieben – auf Kommunikationsobjekte $< i, \texttt{return} >$ und $< i, k >$ für $0 \leq k < n$ auf der einen bzw. $< j, \texttt{return} >$ und $< j, k >$ für $0 \leq k < n$ auf der anderen Seite. Diese entsprechen hier *Argument-Positionen*. Wie bereits

erwähnt, sind diesen Objekten Richtungen des Informationsflusses, wie in der Abbildung oben durch Pfeile angezeigt, zugeordnet.

Für andere Kommunikations-Paradigmen, wie zum Beispiel dem Data Distribution Service (DDS), müssen derartige Kommunikations-Objekte sowie die zugehörigen Abbildungen zwischen diesen Objekten passend definiert werden. Unter Beibehaltung der Grundkonzepte von KIARA sind auch Annotationen, die den Daten zugeordnet sind, denkbar.

Insgesamt bietet die KIARA-Middleware folgende Dienste an:

- Authentifizierung von KIARA Knoten beim Verbindungsaufbau,
- Herstellung eines sicheren Kanals zum Schutz vor Angriffen von außen,
- Verhandlung über die oben umrissene Hinzunahme von Kommunikationsobjekten innerhalb des sicheren Kanals und
- Verschlüsselung (zusätzlich) von bzw. Integritätsschutz von Teilkommunikationen (Feldverschlüsselung).

Im Folgenden werden wir schwerpunktmäßig die beiden letzten Punkte behandeln.

3 Politiken

Erweiterungen des Netzwerks durch Erstellung einer Verbindung oder Hinzunahme von neuen Kommunikationsobjekten zu einer bestehenden sind an Bedingungen geknüpft, die *lokal* verwaltet werden.

Üblicherweise – und auch in KIARA möglich – beziehen sich diese Bedingungen auf Attribute einer nachgewiesenen Identität. Dabei können in diesem Fall *Identitätsattribute* zum Beispiel *Identifikatoren*, *Rollen* oder auch *Vertrauenswürdigkeitsstufen* (engl.: trust levels) sein.

Authentisierung eines über KIARA kommunizierenden Programms kann über externe Dienste vollzogen werden (der FIWARE.OpenSpecification.Security.IdentityManagement Generic Enabler im Falle des EU Future Internet Programms) und das beispielsweise unter Verwendung des Standards OpenID und OAuth. OpenID ermöglicht es einer Komponente ihre eigene Identität einer anderen Komponente mittels einer anerkannten Authentisierungsinstanz zu belegen. OAuth ist ein Authorisations-Standard, welcher für Clients Funktionalitäten zur Verfügung stellt, die – im Namen des Besitzers einer Ressource – Zugriff auf diese Server-Ressource erlauben.

Im Projekt *Assert4SOA*, [Asse], wurden maschinenlesbare (Sicherheits-) Zertifikate untersucht. Diese beschreiben garantierte Sicherheitseigenschaften und auch Maßnahmen bzw. Möglichkeiten zum Nachweis derselben.

Der neue Ansatz von KIARA besteht darin, das (Sicherheits-) Verhalten eines Knoten durch lokale Politiken festzulegen und – mindestens prinzipiell – damit auch nach außen zu beschreiben. Die Regeln von Politiken formulieren neben Bedingungen an die Identität Anforderungen an Sicherheitsannotationen von Kommunikationsobjekten der Gegenseite. In der Implementierung wird zu diesem Zweck die Sprache XACML [OASI] verwendet, wobei *Annotationen* durch Objektattribute in einer jeweils zu fixierenden Sprache beschrieben werden.

Wir betrachten Annotationen als Sicherheits-*Garantien* der (potentiellen) Kommunikationspartner. Sie drücken Sicherheitseigenschaften aus, die an die entsprechenden Kommunikationsobjekte und damit an spezielle Dienste gebunden sind.

Ihre Syntax ist spezifisch für eine spezifische (XACML) Sprache. Gegenwärtig verwenden wir vor allem *Vertraulichkeits-* und *Integritäts-*Annotationen.

Abbildung 3 zeigt eine Situation, wie sie für Vertraulichkeit typisch ist. Forderungen der lokalen Politiken $P1$ und $P2$ beziehen sich auf exportierte Daten. Die gemäß der jeweiligen Kommunikationstechnik zugeordneten Objekte auf der anderen Seite müssen über Annotationen verfügen, die diese Forderungen erfüllen. Im einfachsten Fall geht es um die Zugehörigkeit zu Sicherheitsbereichen (Domains). Weitergehend können bestimmte Ausnahmen von diesen – meistens zu strengen – grundsätzlichen Regeln festgehalten werden. Im allgemeinsten Fall kann der Vergleich im Überprüfen einer Implikation zwischen zwei formalen Ausdrücken bestehen.

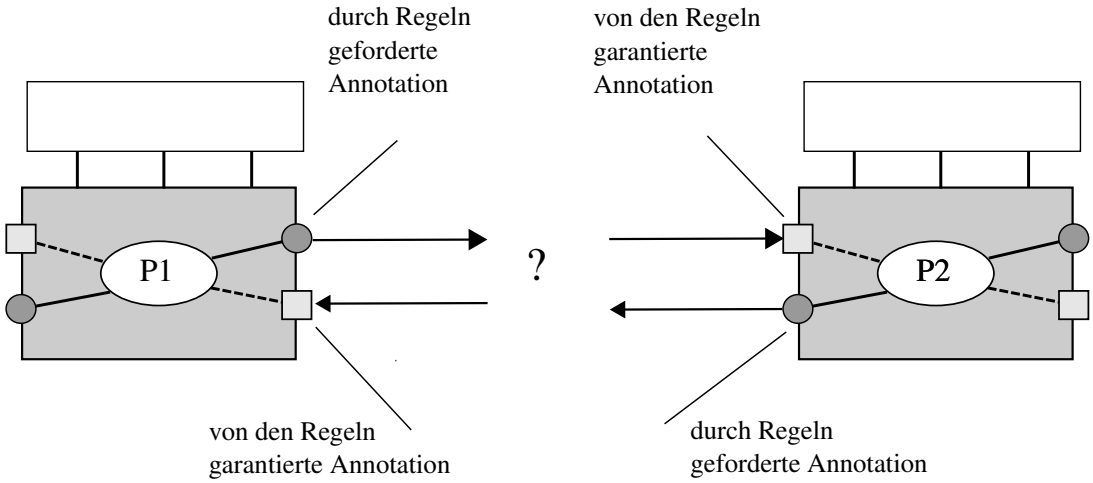

Abb. 3: Verhandlung zwischen Knoten über die lokalen Politiken

Gleichsam als generische Ausnahme können Politiken die *Verschlüsselung* von Daten, die von a an ein Objekt von b geschickt werden, erzwingen. Dies ist dann sinnvoll, wenn b nicht hinreichend vertraut wird, die Daten aber (nur) weitergeleitet werden sollen, zusammen mit anderen weniger kritischen.

Diese Art von *Feldverschlüsselung* erlaubt das „Tunneln“ von bestimmten kritischen Daten durch Knoten, denen in Bezug auf diese Information nicht ausreichend vertraut wird. Eine geeignete Schlüsselverwaltung (Schlüsselverteilung) hat dafür Sorge zu tragen, dass die Kommunikationsobjekte an den Enden (eines solchen Tunnels) die (ursprünglich) angeforderten Garantien bereitstellen. Wenn ein Knoten b' beabsichtigt Daten, die durch ein Objekt o empfangen wurden, zu entschlüsseln, muss die Garantie, welche an o gebunden ist, durch den Knoten, der den Schlüssel zur Verfügung stellt, aufgrund der Regeln von a ausgewertet werden.

Im Fall des Integritätsschutzes werden dual MAC Mechanismen eingesetzt.

4 Semantik

Der KIARA Ansatz hat zum Ziel, trotz des lokalen Charakters von Politiken (und Verhandlungen) *globale* Eigenschaften von ganzen Netzwerken garantieren zu können. Hierzu ist es notwendig, (Sicherheits-) Eigenschaften, die durch Annotationen ausgedrückt werden sollen, semantisch zu beschreiben. In Bezug auf Vertraulichkeit und Integrität verwenden wir hierzu ein *Informationsflussmodell*, [Mant03].

Informationsflussmodelle dienen u.a. dazu, die bekannten Bell la Padula und Biba Regeln semantisch zu unterfüttern. In Abbildung 4 gibt es (nur) zwei Bereiche (Domains), einen kritischen (H) und einen unkritischen (L). Bei konkreten Systemen kann man die angedeuteten Regeln interpretieren als Eigenschaften von Zustandsübergängen, die zum Lesen und Schreiben gehören.

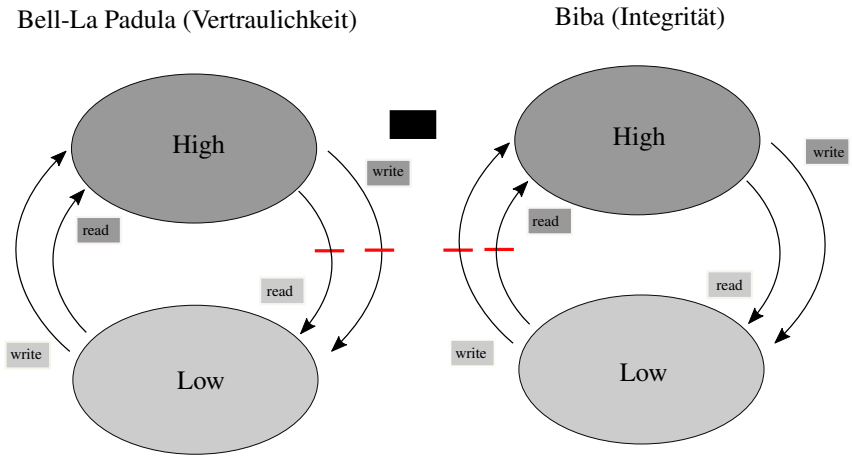

Abb. 4: Bell la Padula und Biba

Dies bedeutet, dass das Sicherheitsverhalten eines Knotens, beschrieben durch seine Politik relativ zu den Forderungen an potentielle Kommunikationspartner semantisch modelliert wird. Damit ist man in der Lage zu definieren, wann Garantien G eines Knotens aus seiner Politik *folgen*. Wann immer $Pol, A \models G$ lokal für alle Knoten gilt, können die Annotationen (Garantien) als *global gültig* angesehen werden.

Im Prinzip würde es somit reichen, dass die beiden Partner sich gegenseitig ihre Politiken präsentieren. Dies ist die KIARA Version von maschinenlesbaren Zertifikaten. Grundsätzlich kann dann $Pol \vdash G$ mechanisch überprüft werden. Es ist zudem sogar möglich, aus Pol *stärkste Garantien* für die Kommunikationsobjekte zu berechnen.

Allerdings ist so etwas im Funktionsumfang von XACML Implementierungen natürlich nicht enthalten. Ein eher konservativer Ansatz besteht darin, die Garantien (als Attributwerte) vorzugeben und die Frage der Gültigkeit offline zu klären. Siehe hierzu auch die Ausführungen in Abschnitt 6.

Strikte Informationsflussregeln sind in der Realität kaum einzuhalten. Zusätzlich zu der schon genannten Feldverschlüsselung gibt es zwei weitere relevante Ausnahmeregelungen:

- die Verwendung von vertrauenswürdigen Downgradern und
- die Berücksichtigung von (Informationsfluss-) Eigenschaften der Anwendung.

Im letzteren Fall sind diese zusätzlichen Annahmen A als Teil der Politik zu repräsentieren, so dass dann $Pol, A \vdash G$ betrachtet wird.

Insgesamt sehen wir folgende potentielle Elemente von Politiken:

- Informationsfluss (Vertraulichkeit, Integrität)
- Downgrading (Kanalkontrolle)
- Verschlüsselung / MAC (Integritätsschutz)

- Chinese Wall Einschränkungen
- Anonymisierung / Pseudonymisierung
- Technische Aspekte

Bei Ansätzen wie Chinese Wall werden Politiken benötigt, die bestehende Verbindungselemente mit in die Entscheidung einbeziehen.

5 Zusätzliche Maßnahmen

Orthogonal zu den oben beschriebenen Lösungen sind in verteilten Szenarios technische Schutzmechanismen notwendig.

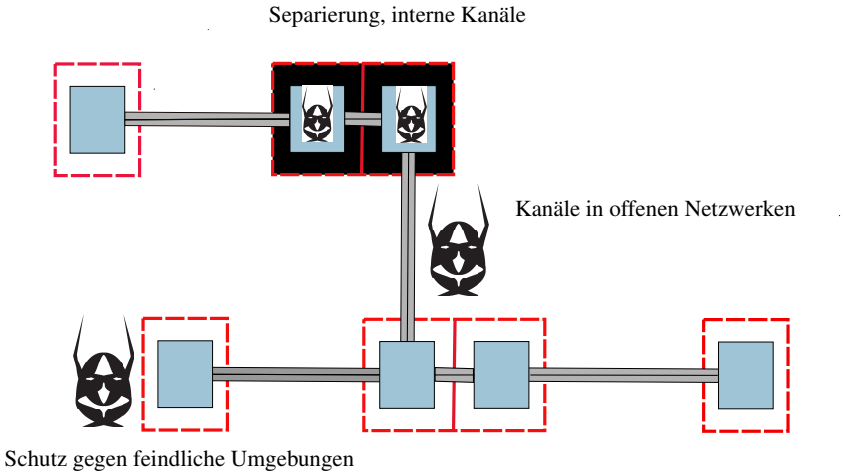

Abb. 5: Technische Schutzmechanismen

Wie in Abbildung 5 dargestellt, betrifft dies:

- die Separierung (Kapselung) von Prozessen,
- die Schaffung sicherer Kanäle in offenen Netzen und
- den Schutz vor feindlichen Umgebungen.

Im Sinne der unten beschriebenen kompositionalen Vorgehensweise ist auch eine Trennung der KIARA Middleware von den jeweiligen Anwendungen notwendig. Die Zertifizierung von Separierungslösungen ist Anliegen des Projektes Euro-MILS, [Euro]. Die Adaption für KIARA ist gegenwärtig in Bearbeitung.

Der Aufbau sicherer Kanäle ist in der KIARA-Implementierung enthalten.

Der Schutz von Komponenten in nicht vertrauenswürdigen Umgebungen ist nur eingeschränkt gelöst. Wir gehen daher davon aus, dass KIARA und gegebenenfalls geeignete Separierungslösungen von unterschiedlich vertrauenswürdigen Instanzen konfiguriert und betrieben werden. Eine grundsätzliche Einschätzung diesbezüglich ist dann Teil der (Verbindungs-) Politiken.

6 Bewertung

Der oben beschriebene KIARA Ansatz folgt im Kern dem Leitgedanken einer *kompositionalen* Vorgehensweise.

Wie im vorangehenden Abschnitt diskutiert verlangen Gesamtlösungen bei strengeren Sicherheitsanforderungen zusätzliche Maßnahmen. Für eine ganzheitliche *Sicherheitsbewertung* eines KIARA-Netzwerks ist eine klare *Trennung der Aspekte (engl.: separation of concerns)* notwendig, die sich auch hier für einen *kompositionalen* Ansatz eignet[1].

Insgesamt ist sicher zu stellen, dass

1. die Sicherheitsmechanismen der KIARA-Middleware konzeptuell adäquat und korrekt implementiert sind,
2. die Anwendungen von der KIARA-Middleware separiert und von anderen Kommunikationskanälen isoliert sind,
3. die Garantien aus den Politiken und Annahmen folgen und
4. die Anwendungen die zusätzlichen Annahmen erfüllen.

Für den Punkt (1) muss die KIARA-Middleware einmal (und nur einmal) bewertet werden. In Bezug auf (2) muss sichergestellt werden, dass die unterliegende Plattform eine Separierung der Anwendungen von der (evaluierten) Middleware erlaubt. Typischerweise wird man in Anwendungsszenarios auch die Möglichkeit, KIARA zu umgehen (eng.: bypass), ausschließen wollen. Wie erwähnt werden existierende Separierungsmechanismen im EU-Projekt Euro-MILS im Hinblick auf eine Zertifizierung untersucht.

Schritt (3) ist für jede Kombination aus (lokaler) Politik und Garantien, die an die Kommunikationsobjekte der Schnittstellen gebunden sind, durchzuführen. Dabei ist zu beachten, dass Politiken und Garantien *deklarativ* gegeben sind und dass es mittlerweile einen starken formalen Hintergrund in Bezug auf Informationsflussanalysen gibt, [Sch].

In Fällen, in denen Informationsflusseigenschaften von Anwendungen mit betrachtet werden sollen, untersuchen wir zurzeit zwei Ansätze:

- die automatische Analyse von Anwendungscode, [SGGH+14] und
- die Verwendung von *Mehrfach-Ausführung, engl.: multi-execution*, [RaSa13].

Unabhängig von Fragen der Evaluierung und Zertifizierung eignet sich der KIARA Ansatz durch seine klare Strukturierung als objektivierter technischer Hintergrund für rechtsgültige Verträge.

7 Zusammenfassung

In diesem Papier haben wir das KIARA Sicherheitsmodell vorgestellt, wie es als Teil des FIWARE Programms der EU konzipiert und implementiert wurde. KIARA ist in den Knoten eines Netzwerks lokalisiert und beruht nicht auf einer zentralisierten Sicherheitskomponente.

Zentrale Merkmale des KIARA Sicherheitsansatzes sind:

[1] Tatsächlich sind wir der Meinung, dass große, heterogene Szenarios (auf die KIARA abzielt) niemals auf monolitische Weise zu behandeln sein werden.

- Komponenten definieren ihr Sicherheitsbedürfnis und, damit verbunden, die Garantien, die sie abgeben können, lokal.
- Die semantische Untermauerung von Politiken und Annotationen erlaubt es, Kriterien für die Überprüfung der (Folgerungs-)Beziehung zwischen lokalen Politiken und Garantien zu definieren, was zu sinnvollen globalen Eigenschaften des gesamten KIARA-Netzwerks führt.
- Bestimmte Sicherheitseigenschaften von Anwendungen, die auf KIARA laufen, können mit berücksichtigt werden.
- Die KIARA Sicherheitsarchitektur ermöglicht eine kompositionale Vorgehensweise bei der Bewertung von Gesamtszenarios.

Literatur

[Asse] Assert4SOA: http://www.assert4soa.eu.

[Blak00] B. Blakley: CORBA Security: An Introduction to Safe Computing with Objects. Addison Wesley (2000).

[Euro] Euro-MILS: www.euromils.eu.

[FIW] https://www.fi-ppp.eu/projects/fi-ware.

[Mant03] H. Mantel: A Uniform Framework for the Formal Specification and Verification of Information Flow Security. Dissertation, Universität des Saarlandes, Saarbrücken, Germany (2003).

[OASI] OASIS: https://www.oasis-open.org/committees/xacml.

[OMG14] OMG: DDS-Security, 1.0 Beta1. Tech. Rep., OMG (2014), .

[RaSa13] W. Rafnsson, A. Sabelfeld: Secure Multi-Execution: Fine-grained, Declassification-aware, and Transparent. *In: CSF '13, Proceedings of the 2013 IEEE 26th Computer Security Foundations Symposium*, IEEE Computer Society Washington, DC, USA (2013).

[Sch] Reliably Secure Software Systems (RS3) - DFG Priority Programme 1496. http://www.reliably-secure-software-systems.de.

[SGGH+14] G. Snelting, D. Giffhorn, J. Graf, C. Hammer, M. Hecker, M. Mohr, D. Wasserrab: Checking Probabilistic Noninterference Using JOANA. In: *it - Information Technology*, 56, 6 (2014), 280–287.