Liste der von C&M zu vergebenden Themen zu Bachelor- und Masterarbeiten

Stand: September 2016

Einsatz einer Internet-der-Dinge-Middleware in der Web-Anwendung SmartCampus (Bachelor- oder Masterarbeit)

Am Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) entsteht gerade eine Middleware, die Anwendungen Funktionalitäten zum Internet der Dinge (Internet of Things, IoT) bereitstellt. Über die Middleware lassen sich flexibel Informationen zu den über das Internet vernetzten Gegenständen abfragen, beispielsweise der Zustand einer Maschine, die Temperatur eines Raums oder der Standort eines Fahrzeugs. Die IoT-Middleware stellt ihre Funktionalität in Form von Web-APIs (Application Programming Interface) bereit, die gemäß dem Stand der Forschung zu gestalten sind. Damit die IoT-Middleware intensiv genutzt werden kann, muss ein Entwickler einer Anwendung wissen, wie er mit diesen APIs im Rahmen der Anwendungsentwicklung umzugehen hat.

In der Bachelor-/Masterarbeit sind zu der vom IOSB gerade entwickelten IoT-Middleware Web-API-Spezifikationen zu erstellen, die gemäß den in der Forschungsgruppe Cooperation & Management (C&M) Richtlinien aufgebaut sind. Beim Entwurf der APIs ist auf deren möglichst systematische und einfache Einsetzbarkeit durch den Anwendungsentwickler zu achten. Hierzu ist in der Arbeit ein Leitfaden zu erstellen, durch den der Anwendungsentwickler gezielt angeleitet wird. Die Praxistauglichkeit des Leitfadens ist am Beispiel der Web-Anwendung SmartCampus, die gemeinsam von C&M und dem IOSB entwickelt wird, zu zeigen.

Ansprechpartner: Pascal Giessler, Sebastian Abeck

Evaluation möglicher Nutzungsszenerien des OAuth 2.0 Device Flows für Internet-der-Dinge-Szenarien

Das Internet der Dinge (engl. Internet of Things, IoT) und die damit einhergehende Gerätevielfalt stellen Webanwendungen vor neue Herausforderungen. Alltägliche Objekte, wie Autos oder Fernseher, werden smart und können im Namen ihrer Besitzer zu Akteuren werden. Ein aktueller Trend sind dabei Wearables, wie Smart-Watches oder intelligente Kopfhörer, mit denen der Benutzer mit Webanwendungen interagieren möchte. Damit der Benutzer mit diesen Dingen Anwendungen nutzen kann, muss er sie mit seinem Account in der Anwendung anmelden. Diese Authentifizierung gehört zum Bereich des Identitäts- und Zugriffsmanagements (engl. Identity and Access Management, IAM).

Durch die eingeschränkten Eingabemöglichkeiten vieler Geräte werden neue Authentifizierungsmethoden benötigt. Ein derzeit etabliertes Verfahren in Webanwendungen ist dabei der "Device Flow". Das Gerät stellt einen Device-Code dar, den der Benutzer auf einer speziell vorbereiteten Seite der Webanwendung eingibt. Anschließend meldet er sich am System an, wodurch die Webanwendung den Device-Code und somit das Gerät dem Account des Benutzers zuordnen kann; er ist auf dem Gerät angemeldet.

Gemeinsam mit einem Industriepartner sollen für dieses Verfahren passende Nutzungsszenarien identifiziert und beispielhaft umgesetzt werden. Zudem sollen weitere moderne und zukunftsweisende Authentifizierungsverfahren für das IoT in Web-Anwendungen recherchiert und wiederverwendbar als Sicherheitsmuster beschrieben werden.

Ansprechpartner: Roland Steinegger

Systematisches Vorgehen zur Erweiterung einer serviceorientierten Architektur (Masterarbeit)

Eine serviceorientierte Architektur setzt sich aus lose gekoppelten und autonomen Services zusammen, die Dienste für ein oder mehrere Anwendungsfälle bereitstellen. Im Zuge der Zeit können sich neue Anwendungsfälle ergeben, die entsprechend durch Services bereitgestellt werden müssen. Dabei ergeben sich zur Entwurfsphase drei Fragestellungen, die einen wesentlichen Einfluss auf die qualitativen Eigenschaften einer serviceorientierten Architektur haben können. Konkret muss geklärt werden, ob (1) die bereits existierenden Services die Anwendungsfälle abbilden können, (2) die existierenden Services erweitert werden müssen, (3) neue Services entwickelt werden müssen oder ob eine Kombination von (2) und (3) notwendig ist. Um diese Fragestellungen beantworten zu können, muss eine Analyse der Ist-Architektur im Hinblick auf die abzubildenden Anwendungsfälle durchgeführt werden. Unklar ist an dieser Stelle, wie ein systematisches und nachvollziehbares Vorgehen für die Analyse zur Beantwortung dieser Fragestellungen aussieht. So muss bspw. zunächst untersucht werden, wie ein Anwendungsfall konzipiert werden muss, um eine Analyse mit der Ist-Architektur zu ermöglichen. Gleichzeitig muss herausgearbeitet werden, welche Informationen über die Ist-Architektur für die Analyse benötigt werden bzw. wie diese aus bestehenden Entwicklungsartefakten ermittelt werden können. Das entwickelte Vorgehen soll anschließend bei der Entwurfsphase eines neuen SmartCampus-Services angewandt werden, um damit die Tragfähigkeit zu demonstrieren. Bei dem SmartCampus handelt es sich konkret um ein System, das Studierenden, Mitarbeitern und Gästen das Lernen, Lehren und Forschen an Hochschulen vereinfachen soll.
Ansprechpartner: Pascal Giessler, Sebastian Abeck

Entwicklung einer verteilten Zugriffskontrolllösung für die SmartCampus-Webanwendung

Der Einzug smarter Dinge in unseren Alltag schreitet stetig voran. Dieses rasante Fortschreiten des Internet der Dinge (engl. Internet of Things, IoT) stellt Unternehmen, die diese Dinge anbieten, vor neue Herausforderungen. Automobile kommunizieren mit ihrem Hersteller, um dem Besitzer aktuelle Fahrdaten per App anbieten zu können oder sogar die Steuerung einzelner Funktionen per App zu übernehmen. Anfragen der App werden dabei von Backend-Systemen der Unternehmen bearbeitet. Diese benötigen somit eine stark verteilte Infrastruktur, um die Zugriffe mit geringen Antwortzeiten bearbeiten zu können. Trotzdem soll der Zugriff kontrolliert erfolgen und die Sicherheit des Systems gewährleistet sein.
Im Rahmen dieser Arbeit soll diese Problematik an Hand zweier Szenarien, der SmartCampus-Webanwendung und einer Automobilanwendung, genauer betrachtet werden. Die verteilten Anwendungen sollen in bestehende Architekturansätze eingeordnet und wiederkehrende Lösungen sollen in der Form von Architekturmustern beschrieben werden. Das Replizieren von Services über verschiedene Länder ist ein Beispiel eines solchen Musters, das zur Reduzierung der Antwortzeit eingesetzt werden kann.
Ausgehend von dieser Architekturanalyse und dem so gewonnenen Verständnis der Systeme soll anschließend die Zugriffskontrolle genauer betrachtet werden. Eingeordnet werden kann dieses Thema in den Bereich des Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM). Das IAM darf im IoT-Umfeld kein Flaschenhals sein und bedarf somit Mechanismen zur effizienten Überprüfung der Autorisation des Benutzers. OAuth ist im Webumfeld derzeit eine Art de facto Standard für die Zugriffskontrolle. Es stellt allerdings nur einen Rahmen bereit und lässt bei der Umsetzung viele Freiheitsgrade, die großen Einfluss auf eine effiziente Zugriffskontrollentscheidung haben können. Somit sollen weitere Ergebnisse dieser Arbeit sowohl die Identifizierung verschiedener Probleme bei der Zugriffskontrolle mit OAuth im IoT-Umfeld als

auch Lösungsmuster sein. Die Lösungsmuster sollen in ein IAM-Rahmenwerk eingeordnet und deren Anwendbarkeit am Beispiel des SmartCampus gezeigt werden.
Ansprechpartner: Roland Steinegger

Systematische Behandlung von Web-APIs im Umfeld eines Identitätsmanagement-Dienstleisters

Bei der Entwicklung von komplexen verteilten Lösungen zum Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) treten Serviceschnittstellen, die heute meist in Form von Ressourcen-orientierten Web-APIs (Application Programming Interface) vorliegen, an zwei Stellen auf: Zum einen werden Web-APIs in der IAM-Lösung genutzt, um hierüber die erforderlichen Funktionalitäten (Authentifizierung, Autorisierung, Logging) bereitzustellen. Hier stellt sich die Frage, wie das Konzept der Microservice-Architektur für zukünftige IAM-Lösungen genutzt werden kann. Zum anderen muss durch eine IAM-Lösung sichergestellt werden, dass die von den Geschäftsanwendungen bereitgestellten Web-APIs nur von den dazu autorisierten Subjekten genutzt werden. Diese Fragestellung ist Teil des API-Managements in Unternehmen.
In der letzten Zeit haben sich bei der Erstellung von Web-APIs gewisse "Best Practices" herausgestellt, die in der Masterarbeit im Hinblick auf deren Verwendbarkeit für die beiden im IAM-Umfeld auftretenden Einsatzgebiete untersucht werden sollen. Die Untersuchung erfolgt am Beispiel eines konkreten IAM-Dienstleisters. Wesentliche Ergebnisse der Arbeit sind eine Bestandsaufnahme des Einsatzes von Web-APIs bei dem Dienstleister sowie Empfehlungen, an welchen Stellen ein Potential für Verbesserungen im Umgang mit den Web-APIs gesehen wird. Durch geeignete Proof-of-Concept-Lösungen ist das konzeptionell ermittelte Verbesserungspotential praktisch aufzuzeigen.
Die Bereitstellung von schützenswerten Web-APIs führt zu dem Problem, dass der Zugriff auf diese geeignet verwaltet werden muss. Zur Verwaltung von Web-APIs werden bereits Webportale, sogenannte Service Registries, angeboten. Diese ermöglichen Anwendungsentwickler das Erkunden und Testen der Web-APIs. Zukünftig soll es den Entwicklern zudem ermöglicht werden, über das Portal Zugriff auf die Web-API zu erbitten, um die Funktionalität in der eigenen Anwendung zu nutzen. Hierfür soll einerseits das Portal entsprechend angepasst und andererseits die API-Spezifikation um notwendige Ergänzungen erweitert werden.
Ansprechpartner: Pascal Giessler, Roland Steinegger