Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Hausarbeit

Jonas Schäufler

Authentifizierung im Internet der Dinge

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Jonas Schäufler

Authentifizierung im Internet der Dinge

Hausarbeit eingereicht im Rahmen der Grundseminar

im Studiengang Master of Science Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Kai von Luck
Zweitgutachter: Prof. Dr. Tim Tiedemann

Eingereicht am: 31. August 2017

Inhaltsverzeichnis

1 Einführung **1**
1.1 Internet der Dinge 1

2 Szenarien für Authentifizierung im IoT **2**
2.1 Entitäten 2
2.1.1 Authentifizierungsszenarien 3

3 Authentifizierung im IoT **4**
3.1 Zertifikat basierte Authentifizierung 4
3.2 Ortsbasierte Authentifizierung 6

4 Autos im IoT **9**
4.1 Auto als Domäne 9
4.2 Ortsbasierte Authentifizierung 9

1 Einführung

1.1 Internet der Dinge

Diese Arbeit befasst sich mit Authentifizierung im Internet der Dinge (*IoT*). Wobei verschiedene Definitionen für das Internet der Dinge existieren wurde während der deutschen EU-Ratspräsidentschaft im Jahr 2007 folgende Definition aufgestellt [1]:

> *Das Internet der Dinge ist die technische Vision, Objekte jeder Art in ein universales digitales Netz zu integrieren.*

Wie aus dieser Definition hervorgeht umfasst das *IoT* viele Arten verschiedener Komponententypen und Systeme. Für die sichere Verwaltung und Kommunikation dieser Entitäten spielt die gegenseitige Authentifizierung eine wichtige Rolle. Diese Arbeit soll einerseits ein Überblick schaffen, in welchen Szenarien die Authentifizierung im Internet der Dinge eine Rolle spielen, sowie verschiedene Lösungsansätze aus vorangegangenen Arbeiten vorstellen. Im letzten Kapitel wird die Tauglichkeit dieser verschiedenen Konzepte auf das Thema *Automotive Security* besprochen.

Komponenten des Internet der Dinge müssen die Möglichkeit haben sicher zu Kommunizieren. Einerseits bedeuted das die Integrität der Nachrichten zu bewaren als auch die gegenseitige Authentifizierung der Komminkationspartner. Wie schon angesprochen ist es möglich, dass sich die Art der Komminkationspartner sich zwar stark voneinander unterscheiden, jedoch können diese meistens in eine der folgenden Kategorien eingeordnet werden:

- Sensoren
- Aktoren
- Dienste
- Nutzer-Endgeräte

Diese Kategorien werden im folgenden Kapitel (2) näher besprochen als auch verschiedene Szenarien für Authentifizierung im Internet der Dinge vorgestellt.

2 Szenarien für Authentifizierung im IoT

2.1 Entitäten

In diesem Kapitel werden verschiedene Anwendungsfälle vorgestellt bei welchen Authentifizierung im *IoT* eine Rolle spielen. Hierfür werden zu erst die in 3.1 aufgelisteten Begriffe besprochen.

Sensoren

Ein Bauteil das Informationen aus seiner Umgebung aufnimmt und diese in ein elektrisches Signal umwandelt. Hierzu zählen herkömmliche Sensoren die physikalische Größen aus der Umgegbung aufnehmen, wie zum Beispiel Temperatur- Druck- oder Helligkeitssensoren, als auch virtuelle Sensoren welche auf schon digitalisierten Informationen arbeiten und aus diesen neue Messgrößen berechnen.

Aktoren

Ein Bauteil das auf elektrische Signale reagiert. Dies kann eine mechanische Bewegung sein oder anderweitiger Einfluss auf physikalische Größen. Zum Beispiel Steuerungseinheiten eines Elektromotors, einer Licht- oder Klimaanlage.

Nutzer-Endgeräte

Endgeräte, wie Computer, Smartphones oder die Mittelkonsole in einem Auto, bei welchen der Mensch eingaben tätigen kann, stellen die menschliche Komponente im *IoT* dar.

Dienste

Nutzer und Dienste sind der Hauptbestandteil des herkömmlichen Netzes wie wir es kennen. Für das *IoT* kommt jedoch hinzu, dass *Sensoren* und *Aktoren* nun Bestandteile als auch Nutzer eines Dienstes sein können.

Wobei die Definitionen für die *Sensoren* und *Aktoren* ursprünglich aus der *Sensorik* und *Antriebstechnik* beziehungsweise *Regelungstechnik* stammen, sind diese auch in diesem Gebiet gültig. Im Kontext des *IoT* handelt es sich bei den *elektrischen Signalen* im Endeffekt um Nachrichten welche Entitäten des *IoT* miteinander austauschen.

2.1.1 Authentifizierungsszenarien

In diesem Abschnitt werden Anwendungsfälle vorgestellt bei welchen eine Authentifizierung zwischen den Entitäten notwendig ist um die Sicherheit des Gesamtsystems zu erhöhen.

Dynamisches Sensornetzwerk

Ein dynamisches Sensornetzwerk beschreibt ein Netzwerk in welchem Sensoren dem Netzwerk beitreten und wieder verlassen können. Dies können mobile Sensoren sein welche ihre Daten abhängig von ihrer Position an verschiedene Dienste senden. Zum Beispiel ein Auto dessen Sensoren seine Daten an das zu seiner Position zugeordnete Netzwerk sendet. Hier muss sich der Sensor gegenüber des Dienstes authentifizieren um das Einspeisen von manipulierten Daten zu verhindern. Sendet der Sensor vertrauliche Daten muss sich auch der Dienst seine authentizität Beweisen können.

Aktoren und Dienste

Wie in Abschnitt 2.1 beschrieben können auch Aktoren Teil eines Dienstes sein. Wenn ein Dienst einen seiner Aktoren ansteuert, muss dieser sich ihm gegenüber authentifizieren um zu verhindern das ein Aktor unautorisiert angesteuert werden kann.

Endnutzer

Aus dem Web ist man mit der Authentifizierung bei Diensten als Nutzer vertraut. Für das *IoT* kommt hinzu, dass Nutzer auch auf Sensoren und Aktoren zugreifen können. Dieser Zugriff wird meist indirekt durch einen zentalen Dienst hergestellt welcher für die Verwaltung der Entitäten zuständig ist. Es kann jedoch auch vorkommen, dass Endgeräte des Nutzers direkt auf Sensoren und Aktoren zugreifen.

3 Authentifizierung im IoT

3.1 Zertifikat basierte Authentifizierung

Um eine sichere Kommunikation für das *IoT* zu ermöglichen wird derzeit daran gearbeitet vorhandene Protkolle zu erweitern. Aktuell handelt sich sich dabei meist um Implementierungen mit symmetrischen Schlüsseln oder Public Keys ohne Zertifikat. Hummen et al. publizierten in *Towards Viable Certificate-based Authentication for the Internet of Things* [2] ein Konzept. mit einer Zertifikatbasierten Authentifizierung basierend auf Datagram TLS.

Außer für die Authentifizierung für die Kommunikation zwischen den Entitäten bringen Zertifikate den Vorteil, dass kompromitierte Entitäten die nicht länger authorisiert sind einfacher außgeschlossen werden können. Außerdem können Entitäten netzwerkübergreifend authentifiziert werden. Und es ist schon eine entsprechende Infrastruktur vorhanden, da im herkömmlichen Internet die verwendung von Zertifikaten weit verbreitet ist.

Da Entitäten des *IoT* aus wenigen kleinen Bauteilen bestehen können sind oft nur schwache Prozessoren vorhanden und die Kapazität von volatilem und persistentem Speicher sehr begrenzt. Die validierung langer Zertifikatketten und deren Übertragung erhöht zudem den Energieverbrauch der Hardware bedeutsam.

In Abbildung 3.1 ist das Netzwerkszenario dargestellt. Zwei *IoT* Domains sind durch Gateways mit dem Internet verbunden. Diese können untereinander kommunizieren und auch das Service-Backend im Internet erreichen.

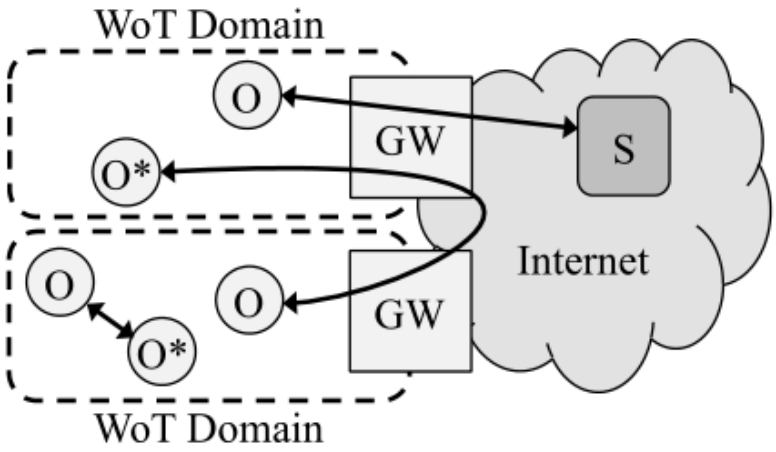

Abbildung 3.1: Netzwerkszenario in [2]

Es werden folgende Mechanismen vorgeschlagen um den Overhead der Übertragung und die Resourcen-Anforderungen an die Entitäten zu verringern:

Pre-validation at the Gateway

Kommuniziert eine Entität über ihre *IoT* Domain hinaus (O mit O* in 3.1), wird die Validierung und Verifizierung der Zertifikatketten auf das Gateway ausgelagert. Dies verringert den Kommunikationsoverhead sowie die Speicheranforderungen der *IoT* Entitäten.

Session Resumption

Beide Verbindungspartner speichern Sitzungsinformationen um die die Anzahl aufwendiger Operationen während des Handshakes bei wiederholtem Verbindungsaufbau zu minimieren.

Handshake Delegation

Die in den vorangegangenen Abschnitten beschriebenen Mechanismen verringern zwar den Overhead verlangen jedoch immernoch das eine *IoT* Entität genug kryptographische Funktionalität besitzt um einen initialen Handshake durchzuführen. Für Objekte mit stark eingeschränkten Resourcen könnte dies eine zu hohe Anforderung sein.
Durch *Handshake Delegation* ist eine Zertifikatbasierte Authentifizierung möglich, ohne dass Kryptographische Funktionen bezüglich Zertifikat oder Public Key auf der Entität vorhanden sein müssen. Der Initiale wird Handshake auf einen Dienst ausgelagert (siehe 3.2). Dieser

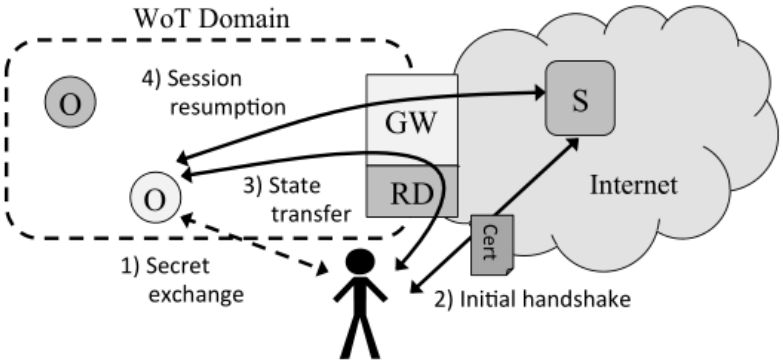

Abbildung 3.2: Netzwerkszenario in [2]

überträgt die Sitzungsinformationen mit der gewünschten Entität. Durch *Session Resumption* kann nun die Verbindung zur *Entität* aufgebaut werden. Dieser Mechanismus setzt voraus dass der Initator ein *shared secret* mit der gewünschten *Enität* besitzt und diese beim Service identifizieren kann.

Implizite Zertifikate

An Ha et al. stellen in [3] ein Protokolldesign vor, das DTLS mit Impliziten Zertifikaten (*ECQV*) erweitert. Implizite Zertifikate sind minimale Zertifikate, ohne komplette Zertifikate oder Public-Keys der CA, welche eigentlich bei einer normalen überprüfung des Zertifikats *explizit* validiert werden. Stattdessen wird mittels Elliptische-Kurven-Kryptografie (*EEC*) aus dem minimierten Zertifikat der *Public-Key* abgeleitet. Eine Nachricht die mit diesem Public-Key verschlüsselt ist impliziert die authentizität des Absenders. Dies erlaubt das Senden von Nachrichten ohne eine explizite überprüfung der Zertifikate der CA.

3.2 Ortsbasierte Authentifizierung

Kapitel 3.1 beschäftigt sich mit Erweiterungen für etablierte Protkolle wie DTLS um diese für das *IoT* tauglich zu machen. Und kann auf alle im Abschnitt 2 angesprochen Szenarien angewendet werden. Eine Authentifizierungsmethode welche sich aus der allgegenwärtigkeit des *IoT* ergibt, ist die *ortsbasierte Authentifizierung* wie sie von Agadakos et al. in [4] beschrieben wird. Hierbei geht es nicht um Authentifizierung auf Entitätenebene sondern der Authentifizierung von Personen an Schlössern mit Terminals, Biometrischen Scannern oder Magnetkartenschlössern. Um unautorisierten Zugang zu einem Ort zu verhindern.

Entitäten des *IoT* und sind überall im Alltag zu finden und wir interagieren täglich mit ihnen. Dies macht sich die in [4] vorgestellte Architektur zu nutze, um ein Modell der Nutzerposition und Bewegung zu erstellen um diese bei der Authentifizierung zu berücksichtigen.

Für die in [4] vorgestellt Architektur (siehe 3.3) gelten die folgenden Definitionen:

1. *Trinkets* Die Entitäten des *IoT* im engeren Sinne, Endgeräte die an das Internet angebunden sind.
   (Smartphones, Autos, Laptops, et cetera.)

2. *Fragments* Engeräte die nicht an das Internet angebunden sind.
   (Laufuhren oder sonstige *smart wearables*)

3. *Tokens* Gegenstände welche keine Verbindung zum Internet aufbauen aber deren Zustand mit Hife eines anderen Endgeräts geteilt werden kann.
   (Magnetkarten, RFID Chips)

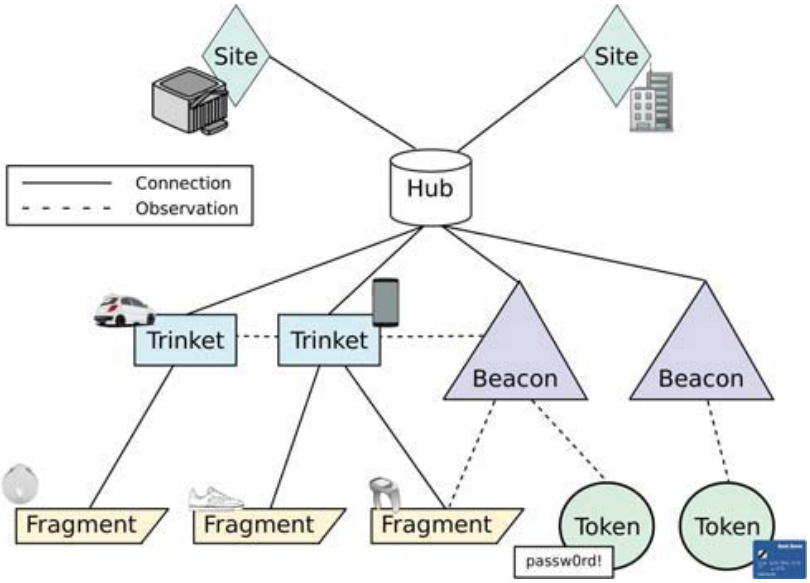

Abbildung 3.3: Architektur (Icarus) aus [4]

Trinkets, *Fragments* und *Tokens* sind einem Nutzer zugeordnet und meldet ihre Position über *Beacons* an den Hub weiter. Dieser bildet diese Informationen auf den *Avatar* des Nutzers ab welcher die Wahrscheinlichkeit für einen Aufenthaltsort darstellt. Bei einem Authentifizierungsversuch kann nun beim Hub überprüft werden wie Wahrscheinlich die authentizität des Nutzers, basierend auf seiner Position, ist.

In wie weit die Position eines *Devices* die authentizität des zugeordneten Benutzers vorhersagen kann kann sich stark unterscheiden. Zum Beispiel ist es wahrscheinlicher, dass ein Nutzer sein Auto an eine andere Person verleiht, als dass eine andere Person mit der Bankkarte des Nutzers Geld abhebt. Um dies zu berücksichtigen wird jedem *Device* ein sogenannter *Device Credit* vergeben, welcher der Gewichtung des *Devices* bei der Berechnung des Avatars entspricht.

4 Autos im IoT

Um einen Eindruck zu bekommen was ein heutzutage produziertes Autos im Kontext des *IoT* bedeuted, zeigt Abbildung 4.1 einen Auszug aus einer Liste mit Sensoren die in einem Auto verbaut sein können. Will man in Zukunft das Auto als Informationsquelle im Kontext des *IoT* nutzen muss ein Konzept entwickelt werden, um diese Systeme und deren Kommunikation abzusichern.
Angriffe auf Informationssysteme im Auto sind aktuelles Thema in der Industrie und Wissenschaft [5]. Die Folgen solcher Angriffe können verheerend sein und eine Bedrohung für die körperliche Sicherheit der Menschen in und um das Auto herum darstellen.

4.1 Auto als Domäne

Betrachtet man ein Auto als *IoT* Domäne wie sie in Abbildung 3.2 abgebildet ist, sind die in Kapitel 3.1 besprochenen Mechanismen um eine *zertifikatbasierte Authentifizierung* realistisch zu gestalten durchaus anwendbar. Dies setzt jedoch nicht nur voraus dass ein *Gateway*, welches diese Verfahren implementiert, im Auto verbaut ist, sondern auch dass die Kommunikation unter den einzelnen Teilsystemen (Sensoren und Aktoren im Auto), sowie die Architekturen dieser, mit einer derartigen Gateway-Architektur kompatibel ist und unter berücksichtigung dieser entwickelt wurde.
Dies verdeutlicht auch wie schwer es ist ein System, das nicht mit Anforderungen an Sicherheit entwickelt wurde, im nachhinein sicher nach außen zu führen.

4.2 Ortsbasierte Authentifizierung

Abgesehen davon dass ein Auto bei der *ortsbasierten Authentifizierung*, wie sie in Abschnitt 3.2 beschrieben ist, ein Trinket darstellt, kann dieses Konzept auch beim Automobil selbst angewendet werden. Zum Beispiel um sicherzustellen dass sich das Auto bei einem Softwareupdate oder Wartung bei einer authorisierten Werkstatt befindet, oder gar um dem Fahrer die Türe zu öffnen.

FUNCTION	BODY SENSOR	PRODUCTION STATUS*
SAFETY		
Air Bag Actuation	Crash Deceleration	major
	Vehicle Rollover (Lateral Acceleration plus Roll Rate)	R&D
	Seat-Belt-Use Buckle Status	limited
	Pressure (Side Impact)	limited
Seat Belt Locking	Vehicle Deceleration	major
	Webbing Payout Velocity	limited
Seat Occupancy	Seat Pan Bladder Pressure	R&D
	Seat Pan Load/Deflection	R&D
Occupant Presence/Pre-Crash Position	Passive Infrared Imaging	R&D
	Ultrasonic Imaging	R&D
	Machine Vision	R&D
Parking/Reversing Aid	Ultrasonic Array	major
	Wide-Beamwidth Radar	limited
Blind Spot Surveillance	Wide-Beamwidth Radar	limited
	Multi-Beam Infrared Laser Array	R&D
Lane Departure	Machine Vision	limited
Night Vision	Passive Infrared Imaging	limited
	Active near-IR Illumination	R&D
INTELLIGENT TRANSPORTATION		
Adaptive Cruise Control	Millimeter Wave Radar	limited
	Infrared Laser Radar	limited
Lateral Lane Guidance	Machine Vision	limited
	Magnetometers	R&D
Behavioral	Driver Condition/Impairment	R&D
NAVIGATION		
Absolute Position	Global Positioning	limited
Autonomous Navigation	Wheel Motion (to zero-speed)	limited
	Vehicle Yaw Rate (high resolution)	limited
COMFORT AND CONVENIENCE		
Convenience	Auto Dimming Mirror	major
	Twilight	major
	Nighttime Headlight Beams	limited
	Seat Pressure/Force Array	limited
Climate	Temperature	major
	Solar Radiation	major
	Humidity	limited
	Ambient CO, NO_x, CH_4 conc.	limited
	Rain/fog/moisture	limited
A/C Compressor Control	Pressure	major
	Temperature	major
SECURITY		
Anti Vehicle Theft	Vehicle Tilt	limited
Anti Intrusion	Vibration	limited
	Ultrasonic Interior Motion Detect	R&D

* Sensor production status rankings are based on the judgment of the author.

Abbildung 4.1: geläufige *Body Sensors* aus **carsense**

Literatur

[1] Deutscher Bundestag, *Aktueller Begriff: Internet der Dinge*, 2012.

[2] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza und K. Wehrle, "Towards viable certificate-based authentication for the internet of things", in *Proceedings of the 2Nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy*, Ser. HotWiSec '13, Budapest, Hungary: ACM, 2013, S. 37–42, ISBN: 978-1-4503-2003-0. DOI: 10.1145/2463183.2463193.

[3] D. A. Ha, K. T. Nguyen und J. K. Zao, "Efficient authentication of resource-constrained iot devices based on ecqv implicit certificates and datagram transport layer security protocol", in *Proceedings of the Seventh Symposium on Information and Communication Technology*, Ser. SoICT '16, Ho Chi Minh City, Vietnam: ACM, 2016, S. 173–179, ISBN: 978-1-4503-4815-7. DOI: 10.1145/3011077.3011108.

[4] I. Agadakos, P. Hallgren, D. Damopoulos, A. Sabelfeld und G. Portokalidis, "Location-enhanced authentication using the iot: Because you cannot be in two places at once", in *Proceedings of the 32Nd Annual Conference on Computer Security Applications*, Ser. ACSAC '16, Los Angeles, California, USA: ACM, 2016, S. 251–264, ISBN: 978-1-4503-4771-6. DOI: 10.1145/2991079.2991090.

[5] A. Humayed und B. Luo, "Cyber-physical security for smart cars: Taxonomy of vulnerabilities, threats, and attacks", in *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*, Ser. ICCPS '15, Seattle, Washington: ACM, 2015, S. 252–253, ISBN: 978-1-4503-3455-6. DOI: 10.1145/2735960.2735992.

[6] W. J. Fleming, "Overview of automotive sensors", *IEEE Sensors Journal*, Jg. 1, Nr. 4, S. 296–308, Dez. 2001, ISSN: 1530-437X. DOI: 10.1109/7361.983469.

[7] A. Compagno, M. Conti und R. Droms, "Onboardicng: A secure protocol for on-boarding iot devices in icn", in *Proceedings of the 3rd ACM Conference on Information-Centric Networking*, Ser. ACM-ICN '16, Kyoto, Japan: ACM, 2016, S. 166–175, ISBN: 978-1-4503-4467-8. DOI: 10.1145/2984356.2984374.

[8] X. Li, H. Wang, Y. Yu und C. Qian, "An iot data communication framework for authenticity and integrity", in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, Ser. IoTDI '17, Pittsburgh, PA, USA: ACM, 2017, S. 159–170, ISBN: 978-1-4503-4966-6. DOI: 10.1145/3054977.3054982.

[9] L. Barreto, A. Celesti, M. Villari, M. Fazio und A. Puliafito, "An authentication model for iot clouds", in *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015*, Ser. ASONAM '15, Paris, France: ACM, 2015, S. 1032–1035, ISBN: 978-1-4503-3854-7. DOI: 10.1145/2808797.2809361.