Internet of Everything

Gedächtnisprotokoll vom 25. Februar 2019

Note: 1,3

1 Allgemeines

Frage: Was ist das Internet of Everything?
Antwort: Formal: Das Zusammenspiel von Personen, Prozessen, Geräten und Daten. Beispielsweise ein Sensor-Aktor Netz, in Form von Home-Automation, Gewächshaussteuerung, usw...
Frage: Kennen Sie einen Anwendung davon hier in Karlsruhe?
Antwort: In Planung befindet sich ein Monitoring-Programm, das die Füllstände der Mülltonnen überwachen soll, sodass diese bei Bedarf außerplanmäßig geleert werden können.
Frage: Jetzt haben wir viele Vorlesungen über das Internet. Was rechtfertigt denn die Existenz dieser Vorlesung, Internet of Everything?
Antwort: Im Internet of Everything kommen andere Faktoren dazu. Geräte haben stark beschränkte Ressourcen, es werden unter Umständen stark persönliche Daten aufgezeichnet, wir haben ein anderes Angreifermodell, das Netz ist selbsorganisiert, es gibt keine zentralen Vertrauensanker und es wird (fast) immer das Funkmedium zur Kommunikation genutzt.

2 LoRaWAN

Frage: Was ist LoRaWAN
Antwort: Die Umsetzung eines zum bereits bestehenden Funknetz parallel existierenden Netzes, das für IoE optimiert ist.
Frage: Können Sie da ein Beispiel nennen?
Antwort: SwissCom. Ein Sensor-Aktor-Netz in der Schweiz, das Hirten ermöglicht, ihre Herde remote zu verfolgen o.Ä.
Frage: Können Sie mir die Infrastruktur eines LoRaWANs aufzeichnen.
Antwort: Ja. Diese besteht aus Funkmasten, die mit den Endgeräten kommunizieren. Hinter den Masten befinden sich zentrale Server, eventuell Load-Balancer und Application Services.
Frage: Wie hoch ist die Bandbreite des Netzes?
Antwort: 100kbit/s bis 300kbit/s, soweit ich weiß.
Frage: Was gibt es für Möglichkeiten für die Kommunikation zwischen den Geräten und den Masten? Diese haben wir übrigens Gateway genannt.

Antwort: Dort gibt es 3 Level. Level A ist Endgerät-initiiert. Hier erwacht das Endgerät, wenn es zum Mast kommunizieren will. Es wählt zufällig einen möglichen Kanal aus und beginnt unsynchronisiert die Sendung. Der Mast muss dazu permanent auf allen möglichen Kanälen lauschen. Bei Level B existiert dazu noch ein Zeitschlitz für den Masten, zu dem das Endgerät aufwacht und lauscht, ob der Mast sendet. Level C verlangt von beiden Kommunikationspartnern, permanent zu lauschen, sodass zu jedem Zeitpunkt in jede Richtung eine Kommunikation möglich ist.

3 Klassifikationen

Frage: Wir hatten Geräte im IoE klassifiziert. Was können Sie mir dazu sagen?
Antwort: Es gibt zwei vorgeschlagene Kategorien, nach denen man klassifizieren kann. Computation (C0 - C2) und Energy (E0 - E9). C0 sind Geräte, die kaum Bandbreite für die Kommunikation haben, ebenso wenig Programmspeicher und RAM. C1 Geräte haben mehr Programmspeicher und RAM. C2 ist die leistungsfähigste Klasse. E0 Geräte werden mit Energy-Harvesting betrieben, beispielsweise mit Solarzellen. E1 Geräte basieren auf Batterien oder Akkus, die man aufladen oder austauschen kann. E2 Geräte basieren auf Batterien, hier besteht aber keine Möglichkeit, diese auszutauschen. Die Geräte müssen dann ausgetauscht werden. E9 Geräte sind an eine Steckdose angeschlossen.

4 Privatsphäre

Frage: Anfangs haben Sie Privatsphäre erwähnt. Was ist denn das überhaupt?
Antwort: Das ist in unserem Fall der Schutz des Persönlichkeitsrechts bei der Verarbeitung personenbezogener Daten.
Frage: Was haben wir für Schutzziele?
Antwort: Confidentiality, Integrity (stark/schwach), Availability, Unverkettbarkeit, Transparenz, Abstreitbarkeit...
Frage: Wie erreiche ich denn Vertrauligkeit?
Antwort: Mit Verschlüsselung.

5 Schlüsselaustausch

Frage: Wie wird denn im IoE Verschlüsselung umgesetzt?
Antwort: Mit symmetrischer Kryptographie. Beide Kommunikationspartner hüten ein gemeinsames Geheimnis, beispielsweise den gleichen Schlüssel.
Frage: Was haben wir für Möglichkteiten für einen Schlüsselaustausch kennengelernt?
Antwort: Single-Mission-Key. Ist einfach umzusetzen: das Schlüsselmaterial ist

vor Benutzung in die Geräte fest einprogrammiert. Problematisch ist es aber, wenn der Schlüssel nach einem erfolgreichen Angriff veröffentlicht wird, dann ist mein gesamtes System unsicher.
Frage: Was gab es noch für Verfahren?
Antwort: Key Infection und EGLI.
Frage: Was ist EGLI?
Antwort: Ein Schlüsselaustauschverfahren. Jeder Knoten bekommt eine zufällige Untermenge aller Schlüssel. Jetzt besteht die Möglichkeit, dass die Knoten den Index der vorliegenden Schlüssel an seine Nachbarn sendet. Der Empfänger überprüft, ob er einen Schlüssel mit diesem Index gespeichert hat. Dann teilen sie einen Schlüssel und können diesen um Folgenden zur Kommunikation verwenden. Es kann durchaus vorkommen, dass keine gemeinsamen Schlüssel vorhanden sind. Dann ist erstmal keine verschlüsselte Kommunikation möglich. Ein anderer Ansatz wäre es, einen Klartext mit allen vorliegenden Schlüsseln zu verschlüsseln und dann die Klartext-Chiffrat-Paare zu senden. Die Empfänger dekodieren dann mit allen vorliegenden Schlüsseln das Chiffrat und vergleichen es mit dem Klartext. Stimmen diese überein, ist ein gemeinsamer Schlüssel vorhanden. Beide Verfahren sind nicht sicher.

6 Transportverfahren

Frage: Welche Arten von Kommunikationsmuster haben wir kenngelernt?
Antwort: Unicast (P2P), Multicast (P2MP), Concast (MP2P), Anycast.
Frage: Was ist der Unterschied zwischen Broadcast und Multicast?
Antwort: Broadcast adressiert jedes Gerät im Netz. Mulitcast nur eine Teilmenge davon, beispielsweise alle Geräte mit dem Präfix dead:beef:1337::
Frage: Was ist ein Anycast?
Antwort: Ein Kommunikationsmuster, das im Rahmen von ZigBee vorgestellt wurde. Es handelt sich um ein Broadcast in einer Gruppe von Geräten, in der sich der Sender selber nicht befindet. Er startet zunächst einen Unicast zu einem beliebigen Teilnehmer der Zielgruppe, meistens der Nächstgelegene. Dieser startet nach Empfangen der Dateneinheit einen Broadcast innerhalb seiner Gruppe.
Frage: Beim Multicast hatten wir uns ein Protokoll angeschaut. Welches war das?
Antwort: PSFQ.
Frage: Können Sie mir das erklären anhand dieses Beispiels hier auf dem Papier?
Antwort: Ja. Die Wurzel möchte beispielsweise eine Sensorwertabfrage an die Knoten senden. Hierbei ist die Latenz nicht so wichtig, es geht eher darum, dass alle Anfragen auch bei den Knoten ankommen. Die Wurzel "pumptëine Dateneinheit per Broadcast an seine Kindknoten. Diese leiten die Dateneinheit dann wiederum an deren Kinder weiter.
Frage: Wann wird weitergeleitet?

Antwort: Wenn ein Knoten eine neue Dateneinheit in konsistenter Reihenfolge empfängt und diese noch nicht 3 mal gehört, also von anderen Knoten gesendet, wurde.
Frage: Was macht ein Knoten, wenn er feststellt, dass ihm eine Dateneinheit fehlt?
Antwort: Er broadcastet ein NACK. Inhalt des NACKs ist eine Bitmaske, in der für jede fehlende Dateneinheit eine 1 gesetzt wird. Bits die eine logische 0 repräsentieren, stehen für eine nicht fehlende Dateneinheit.
Frage: Was macht ein Knoten, wenn er nun eine Dateneinheit nachgeliefert bekommt?
Antwort: Er broadcastet diese weiter, insofern alle vorherigen Dateneinheiten vorhanden sind, und die neue Dateneinheit nicht öfter als 3 mal gehört wurde.

7 6LoWPAN

Frage: Was ist denn 6LoWPAN?
Antwort: Ein Protokoll zur Anbindung meiner Konten um SAN an das IPv6 Internet.
Frage: Welche Arten von 6LoWPAN Netzen haben wir kennen gelernt?
Antwort: Simple, Ad-Hoc und Extended.
Frage: Können Sie mir die Topologie eines simple 6LoWPAN aufzeichnen?
Antwort: Ja. Ein 6LoWPAN-Edge-Router verbindet das IPv6 Internet mit 6LoWPAN Router-Geräten. Darunter befinden sich 6LoWPAN Hosts.
Frage: Können Sie mir den Protokollstack im Edge-Router aufzeichnen?
Antwort: Ja. Auf der linken Seite haben wir herkömmliche Protokolle: Ethernet-PHY, Ethernet-MAC und eben IPv6. Auf der linken Seite kommt 802.15.4 zum Einsatz auf Schicht 1 und 2. Darüber liegt eine Adaptionsschicht von 6LoWPAN, sagen wir sie arbeitet auf Schicht 2,5. Dann auch Schicht 3 haben wir wieder IPv6.