cnlab

IG ICT
INTERESSENGEMEINSCHAFT DER ZÜRCHER GEMEINDEN
FÜR INFORMATION AND COMMUNICATIONS TECHNOLOGY

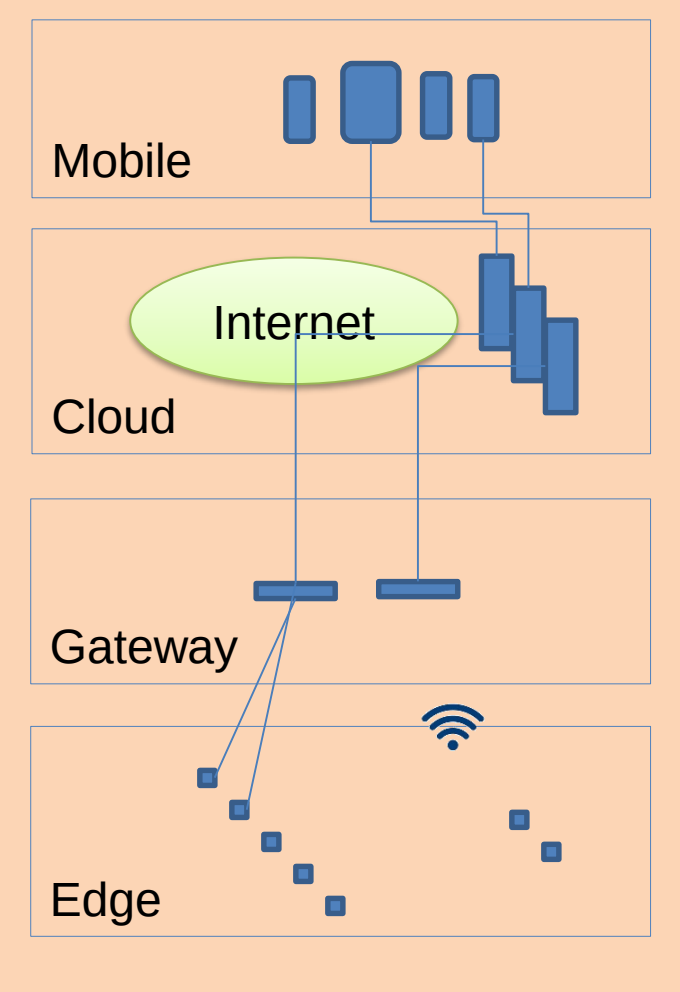
Security of IoT

Generalversammlung
21. März 2017

Agenda

- IoT und Security
- IoT Frameworks
- LoRa Security

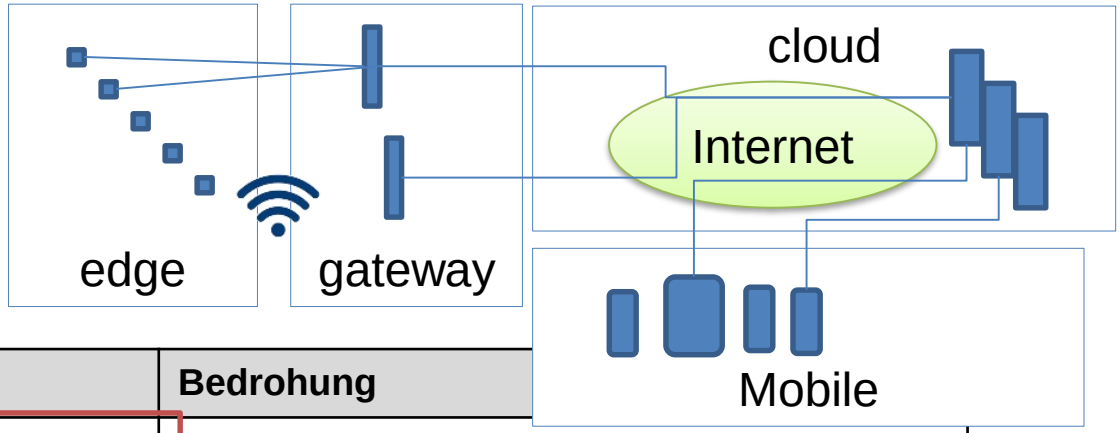
Die OWASP-Sicht



- The **edge** code that runs on actual **IoT devices**. Often times edge components are resource constrained or operate in isolated environments.
- A **gateway** device is often used to aggregate and bridge communications from edge devices.
- The edge, or gateway, will often communicate with some sort of **cloud component**, often a web service. This component could be deployed in a company data center or a public cloud computing environment. The cloud component often supports complex user interfaces, analytics capabilities, and provide access to data aggregation back ends.
- Finally, many IoT ecosystems consist of **mobile application** components that allow users to interact with the ecosystem via smart phones or tablets.

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Angriffsvektoren



Komponente	Zielobjekt	Bedrohung
Edge & Gateways	Daten	Vertraulichkeit
	Funktionen	Einfluss auf «Dinge»
	Credentials	Daten-Integrität
Link Edge→Gateway	Daten	Vertraulichkeit
	Funktionen	
Link Gateway→Cloud	Daten	
	Funktionen	Einfluss auf «Dinge»
Cloud	Daten	Vertraulichkeit
	Funktionen	Einfluss auf «Dinge»
Mobile App	Daten	Vertraulichkeit
	Funktionen	Einfluss auf «Dinge»
	Credentials	Vertraulichkeit, Einfluss auf «Dinge», Integrität

OWASP IoT Top 10 Vulnerabilities

Category	IoT Security Consideration
I1: Insecure Web Interface	Ensure that any web interface coding is written to prevent the use of weak passwords …
I2: Insufficient Authentication/Authorization	Ensure that applications are written to require strong passwords where authentication is needed …
I3: Insecure Network Services	Ensure applications that use network services don't respond poorly to buffer overflow, fuzzing …
I4: Lack of Transport Encryption	Ensure all applications are written to make use of encrypted communication between devices…
I5: Privacy Concerns	Ensure only the minimal amount of personal information is collected from consumers …
I6: Insecure Cloud Interface	Ensure all cloud interfaces are reviewed for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces) …
I7: Insecure Mobile Interface	Ensure that any mobile application coding is written to disallows weak passwords …
I8: Insufficient Security Configurability	Ensure applications are written to include password security options (e.g. Enabling 20 character passwords or enabling two-factor authentication)…
I9: Insecure Software/Firmware	Ensure all applications are written to include update capability and can be updated quickly …
I10: Poor Physical Security	Ensure applications are written to utilize a minimal number of physical external ports (e.g. USB ports) on the device…

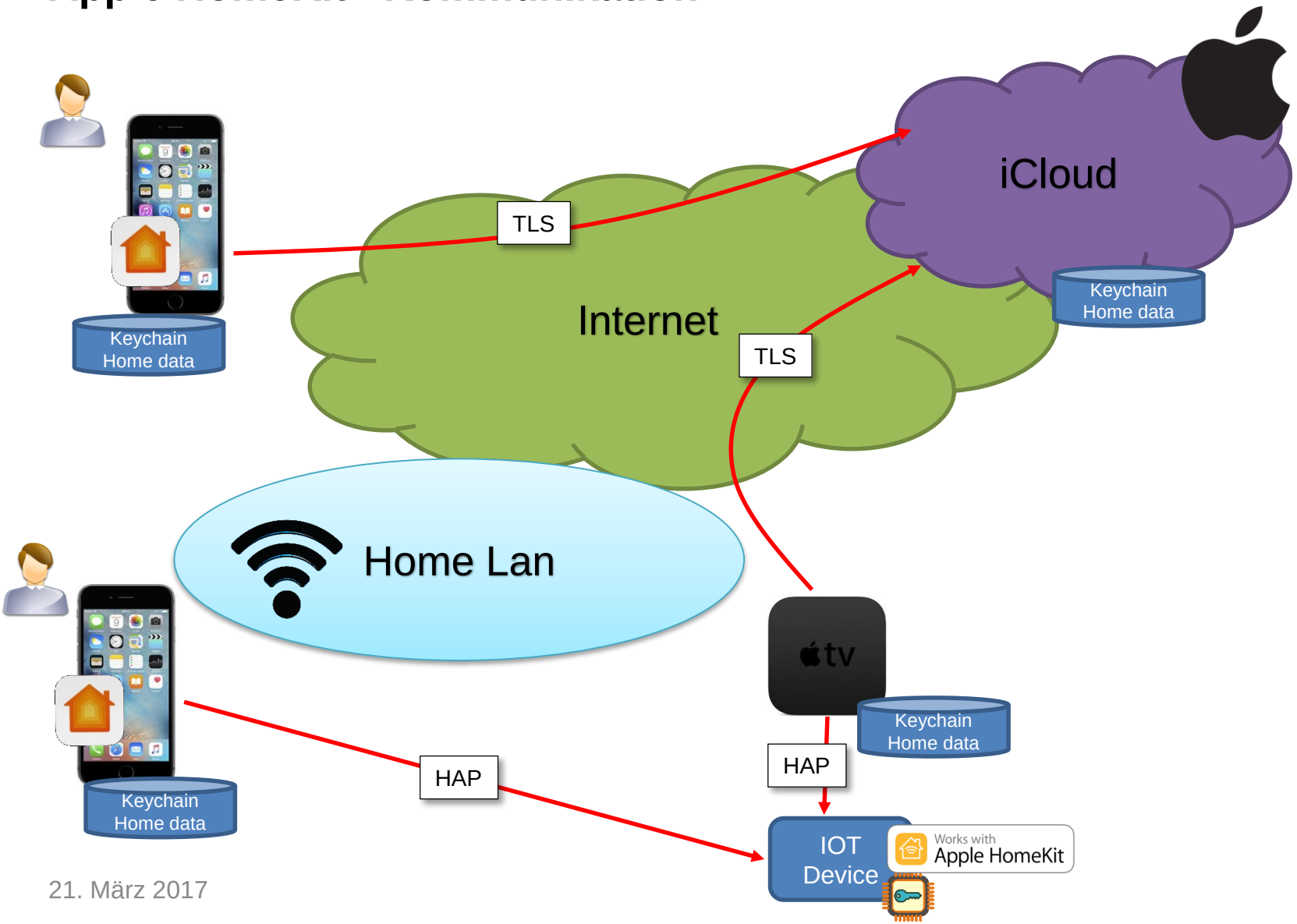
Sicherheit bekannter IoT Frameworks
Apple HomeKit

- Home Automation Framework von Apple
- Datenbank in iOS enthält Informationen über das Haus, Räume, Szenen und IOT-Devices:
  - Licht-Steuerungen
  - Thermostaten
  - Schlösser
  - Storen
  - ....
- Nur MFI zertifizierte Hardware und Firmware sind zugelassen

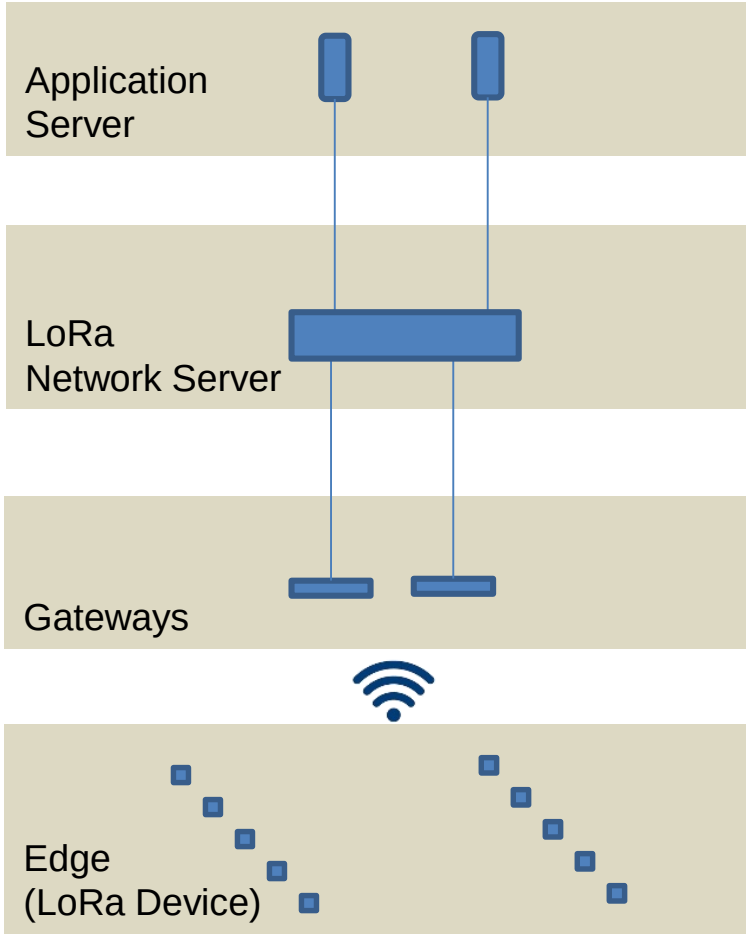
History

- iOS 8 (2014):
  - + Home-Daten
  - + Steuerung via Siri
  - + Remote Control via iCloud und Apple TV
  - + Third-Party-Apps zur Steuerung
- iOS 9 (2015):
  - + Remote Control via iCloud direkt auf Fremd-Geräte
  - + Third-Party-Apps zur Steuerung
- iOS 10 (2016):
  - + Home App von Apple zur Steuerung
  - + Remote Control via iCloud und iPad

Apple HomeKit - Kommunikation



LoRa – Schutzziele und Massnahmen



Vertraulichkeit

Übermittelte Daten müssen vor unberechtigtem Zugang geschützt sein.

Integrität

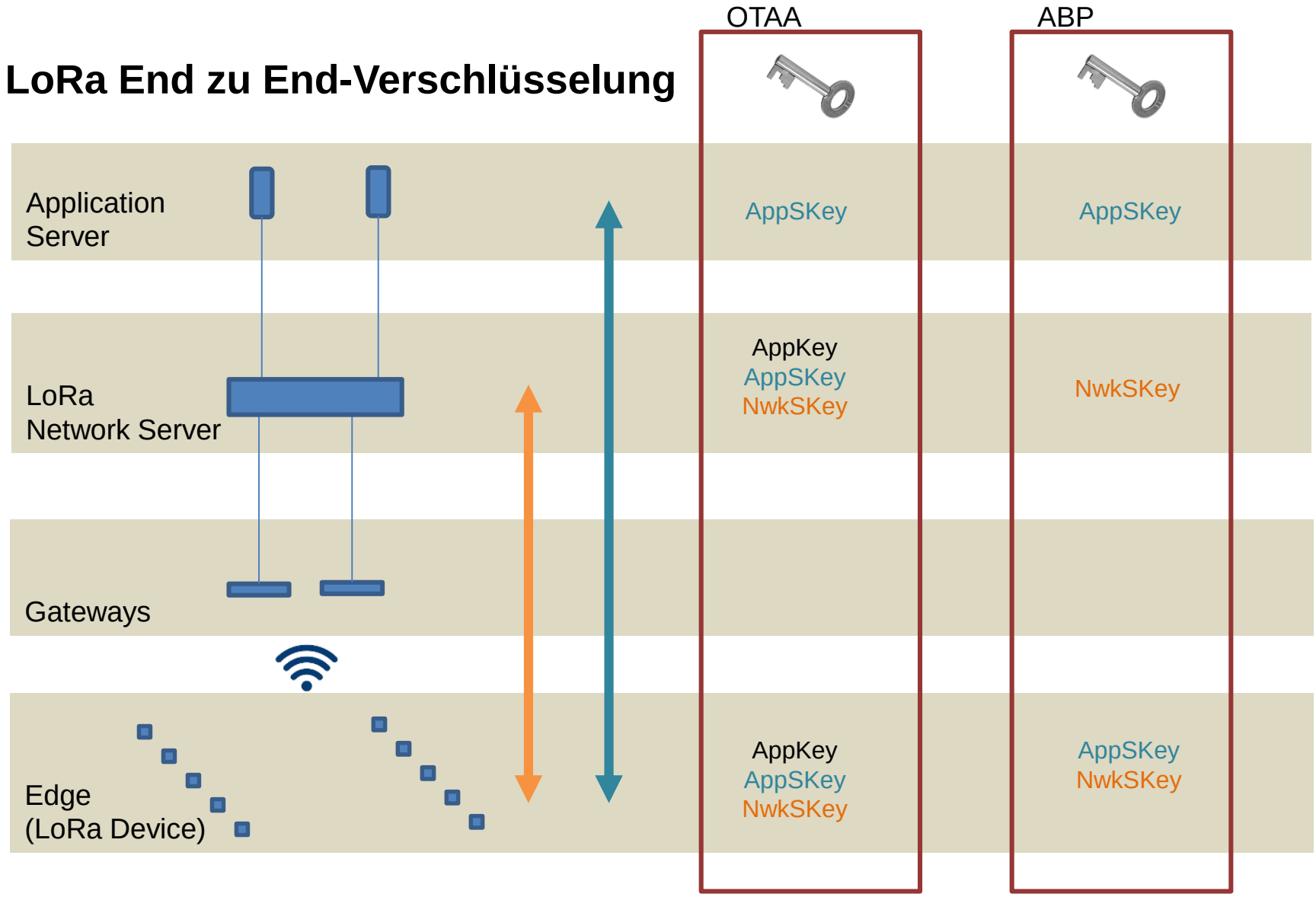
Übermittelte Daten müssen vor unberechtigten Veränderungen geschützt sein.

Authentizität

Echtheit der Daten muss gewährleistet sein.

Verfügbare Massnahme:
End zu End-Verschlüsselung

LoRa End zu End-Verschlüsselung



LoRa-Security

Das LoRa Security-Modell gibt Grundlagen für einen sicheren Betrieb einer IoT-Umgebung. Wichtige Bereiche sind jedoch ungenügend definiert. Dies führt zu unsicheren Implementationen.

- LoRa-Netzwerk-Server-Betreiber haben Zugang auf Schlüsselmaterial. Das gibt Zugang zu den Anwendungsdaten
- Zugang zum Schlüssel in einem Gerät kompromittiert die System-Sicherheit
- Fehlende Definition des Schlüsselmanagements: Schlüssel-Generierung, Speicherung und Erneuerung
- Kompromittierte Schlüssel können nicht sicher aktualisiert werden

Danke

Christian Birchler
christian.birchler@cnlab.ch
+41 55 214 33 40

Links

Organisationen

- https://iotsecurityfoundation.org/
- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/

LoRa

- https://www.thethingsnetwork.org/wiki/LoRaWAN/Security
- https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN_Security-Whitepaper_V6_Digital.pdf