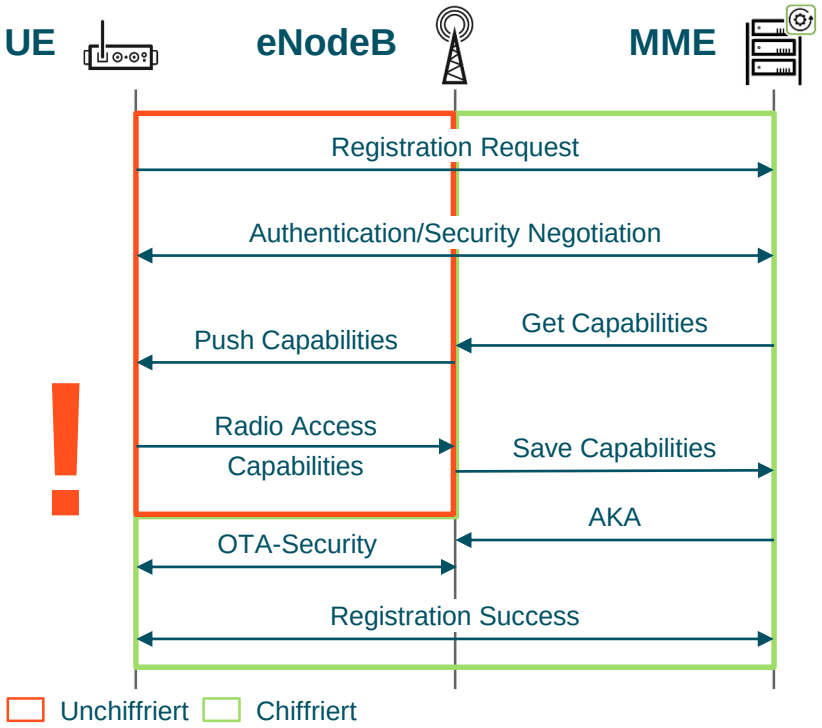
«Angriff auf die Radio-Fähigkeiten von IoT-Geräten – eine Sicherheitsbedrohung?»

Reto Amstad
Senior Security Consultant

Agenda

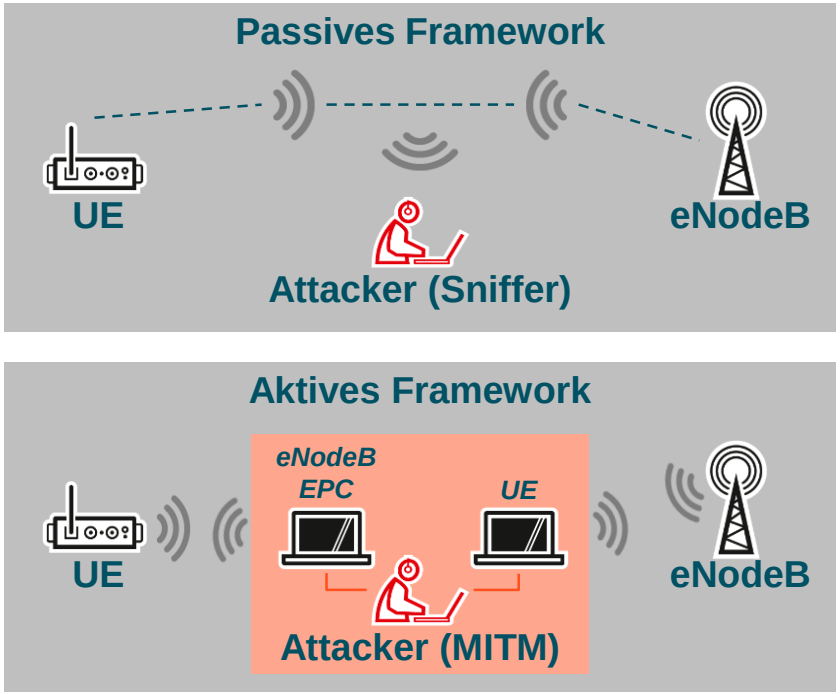
01 – Angriff auf die Radio-Fähigkeit eines IoT-Geräts
02 – Verwendetes Test-Framework
03 – Findings und Auswirkungen
04 – Wird mit 5G alles besser?
05 – Konsequenzen und Handlungsbedarf für (zukünftige) IoT-Geräte

LTE-Registrationsablauf



- Registrierungsprozess wird teilweise klar über Luftschnittstelle (UE – eNodeB) kommuniziert
- UE-Fähigkeiten (Radio Capabilities) werden klar ausgetauscht
- Fähigkeiten werden im Netz für lange Zeit gespeichert

Test-Framework und Komponenten



bladeRF x40 Software Defined Radios von Nuand
(Quelle: www.nuand.com/product/blade-x40)

srsLTE Open Source LTE Stack von Software Radio Systems
(Quelle: https://github.com/srsLTE)

ASN1c Open Source Compiler für ASN1 Industrie Format
(Quelle: https://github.com/vlm/asn1c)

Wireshark Network Protokoll Analyzer
(Quelle: www.wireshark.org/downloads)

QCSuper Open Source um 4G Radio Frame aufzuzeichnen – Qualcom based
(Quelle: https://github.com/P1sec/QCSuper)

Disclaimer

Es ist **strafbar** in einem öffentlichen Telekommunikationsnetz aktive Komponenten einzusetzen!

Bitte verwenden Sie dazu ausschliesslich isolierte Umgebungen!

Findings und Auswirkungen

Sicherheits-Findings	Auswirkung auf das IoT-Gerät
Deaktivierung **PSM** (Power Save Mode) im IoT-NB	Beeinflussung des Batterieverbrauchs
Modifizierung der **Radio-Fähigkeiten,** z.B. Entfernen von Frequenz-Bänder, UE Cat. verändern etc.	«Service Downgrade» oder sogar DoS
Gesteuertes **«Cell hoping»** durch Modifikation der **Sendeleistung** des fake eNodeB (inklusive Nachbarzellen anbieten)	Batterieverbrauch, DoS, Paging flood, chaotischer Zustand

Wird alles besser mit 5G?

Wir glauben **NICHT!**

Liste der gefundenen Angriffe für 5G:

Attack	Vulnerability	Assumption & Validation	New Attack?	Notable Implication
NAS Layer				
Counter reset	Generating/verifying integrity using MAC in sec_mode_command and sec_mode_complete messages	Known C-RNTI [45], MitM relay [28, 45]	Y	DoS, over billing
Uplink NAS Counter Desynchronization	Lack of attempt counter for the security mode command procedure and generating/verifying integrity using uplink counters in sec_mode_command and sec_mode_reject messages	Known C-RNTI [45], MitM relay [28, 45]	Y	Prolonged DoS
Exposing NAS sequnece number	cnt_{ul}^{ue} & cnt_{dl}^{amf} transmitted in plain-text	Known C-RNTI [45], session keys unkown	Y	Service profiling
Neutralizing TMSI refreshement	configuration_update_command may not require acknowledgment	Known C-RNTI [45], old TMSI (Attack 6.3.1), MitM relay [28, 45]	Y	Location Tracking
Cutting of the device using `reg_request`	AMF accepts registration_request without integrity	Know C-RNTI [45]	Y	DoS
Cutting of the device using `ue_dereg_request`	AMF accepts de-registration_request without integrity	Known C-RNTI [45]	Y	DoS
Downgrade using reject messages	No integrity in reject message	Known C-RNTI [45] or TMSI (Attack 6.3.1)	Inspired by [48]. [28]	Downgrade from 5G
Linkability using `authentication_failure`	Different response in MAC failure	Known TMSI (Attack 6.3.1)	Inspired by [11] in 3G and [14] in 5G	Tracking
Paging channel hijacking	No integrity check in paging messages	Known S-TMSI (Attack 6.3.1) or I-RNTI	Inspired by [28]	Stealthy DoS
Panic attack	No integrity check in paging messages	Malicious *gNB* [28, 45]	Inspired by [28]	Atificial chaos, mass victimization
Linkability/Tracking using `sec_mode_command`	Generating/verifying integrity using MAC in sec_mode_command message	Known C-RNTI [45], MitM relay [28, 45]	Inspired by [28]	Tracking
RRC Layer				
Denial of service using `rrc_setup_request`	No integrity in `rrc_setup_request`	Known C-RNTI [45]	Y	DoS
Installing null cipher and integrity	Lack of integrity protection in `rrc_sec_mode_failure`	Known C-RNTI [45], MitM relay [28, 45]	Y	SUPI catching
Lullaby attack with `rrc_reconfiguration`	UE's response to invalid integrity protection to the `rrc_reconfiguration`	Known C-RNTI [45], fake base station [28, 45]	Y	Force state change, battery draining
Lullaby attack using `rrc_reestablish_request`	UE's reaction to invalid integrity protection to the `rrc_reestablish_request`	Known C-RNTI [45], fake base station [28, 45]	Y	Force state change, battery draining
Lullaby attack with `rrc_resume`	UE's response to `rrc_resume`	Known C-RNTI [45], fake base station [28, 45]	Y	Force state change, battery draining
Incarceration with `rrc_reject` and `rrc_release`	rrc_reject is not integrity protected	Known C-RNTI [45] or TMSI (Attack 6.3.1)	Y	DoS
Incarceration with `rrc_reestablish_reject`	rrc_reestablish_reject is not integrity protected	Known C-RNTI [45] or TMSI (Attack 6.3.1)	Y	DoS
Cross Layer Attacks				
Exposing Device's TMSI and Paging Occasion	Lack of acknowledgment of rrc_release & paging retransmissions	Known C-RNTI [45], MitM [28, 45]	Y	Location Tracking, stealthy DoS, downgrade from 5G, artificial chaos, mass victimization
Exposing Device's I-RNTI	Lack of acknowledgment of rrc_release & paging retransmissions	Known C-RNTI [45], MitM [28, 45]	Y	Stealthy DoS

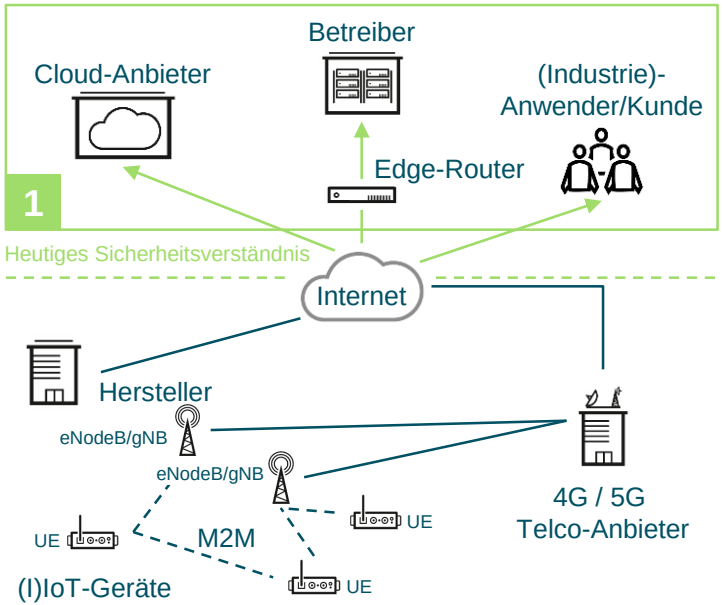
Table 1: Summary of 5GReasoner's findings.

! Downgrade Service, Batterieverbrauch-Thema und DoS sind auch bei 5G möglich!

(Quelle: 5gReasoner: A property-directed Security and Privacy Analysis for 5G Cellular Network Protocol, Syed Rafiul Hussain)

Konsequenzen für das IoT-Ökosystem

(I)IoT-Ökosystem



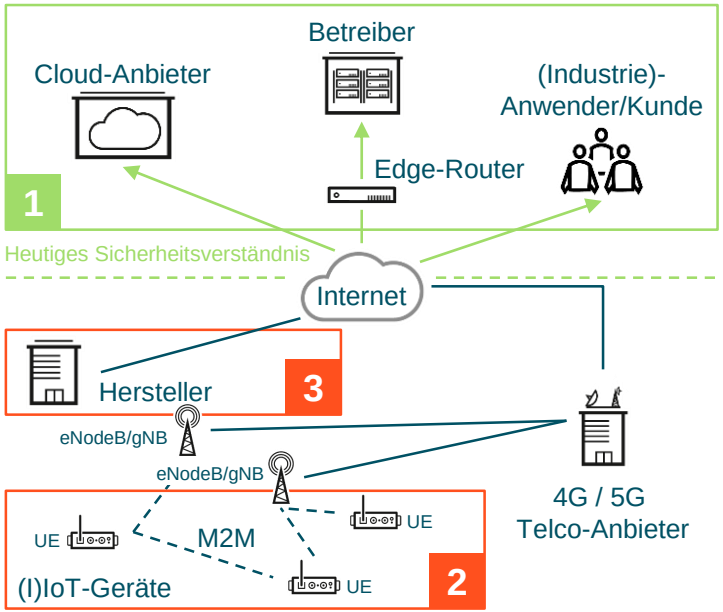
1 IoT-Sicherheit wird heute meistens als Absicherung ab Edge-Router hin zum Betreiber, Cloud-Anbieter oder Anwender gesehen!

Eine fehlende Sicherheitssicht auf die IoT-Peripherie bringt (Cyber-)Risiken:

1. Im Produktionsprozess für den Anwender (Kunde)
2. In der Nachvollziehbarkeit für den Betreiber
3. Für die mögliche Anpassungsfähigkeit aus Sicht Hersteller

Handlungsbedarf für IoT-Ökosysteme

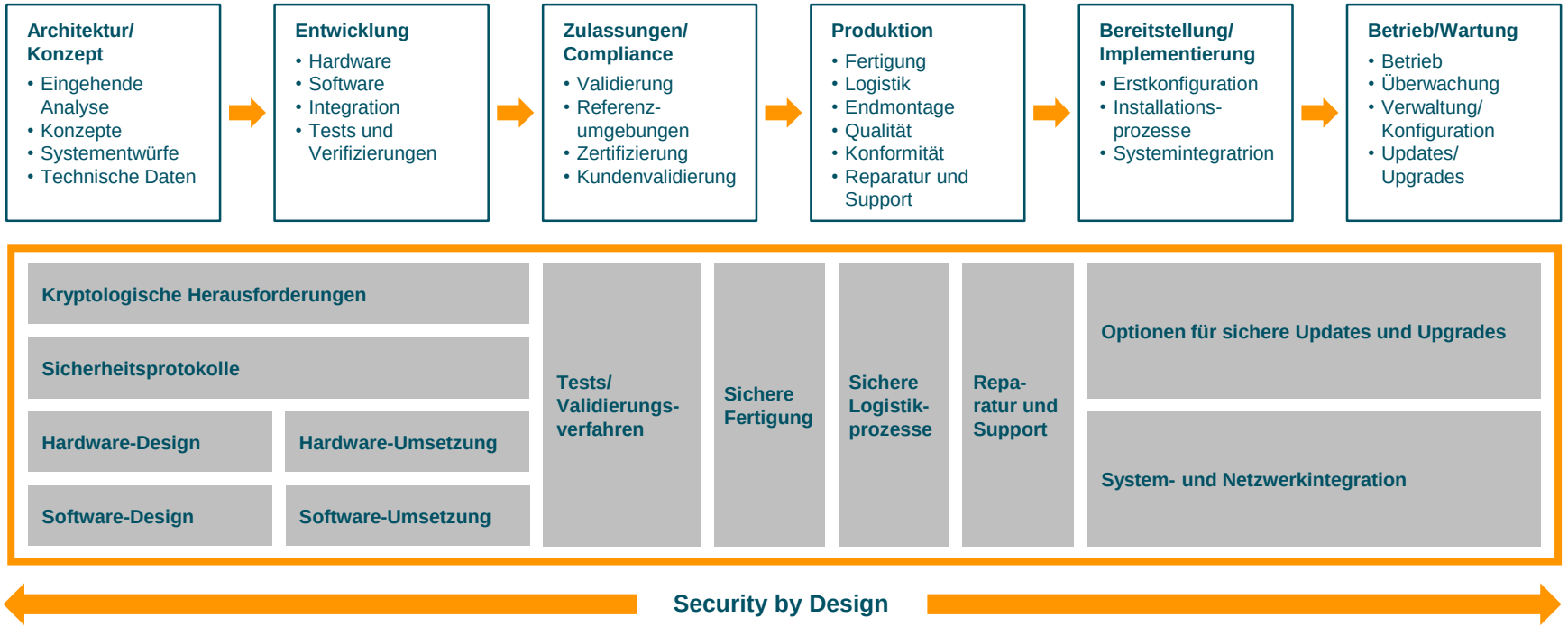
(I)IoT-Ökosystem



2 In einer umfassenden Sicherheit muss das (I)IoT-Gerät auch miteinbezogen werden. Sicheres Architektur- und Softwaredesign mit Validierungen und Plausibilitätsprüfungen sind für das IoT-Gerät Pflicht.

3 Hersteller von IoT-Geräten müssen Geräte entwickeln, welche sich den sich verändernden Cyber-Risiken und Technologieentwicklung anpassen können (Update-Fähigkeit). Schaffen Sie als Hersteller den entscheidenden Wettbewerbsvorteil mit «Security by Design» von Anfang an in der Entwicklung Ihres IoT-Gerätes.

Nachhaltige (I)IoT-Sicherheit – Security-Know-how im Produktlebenszyklus



Sichere Schweiz.
Bit für Bit.

Reto Amstad
Senior Security Consultant
Email: reto.amstad@cyone.ch
Telefon +41 41 748 85 16

cyone.ch