Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Wissenschaft und Technologie

Nutzung der LTE-Technologie in einem militärischen Kontext

Risiken und potentielle Minderungen

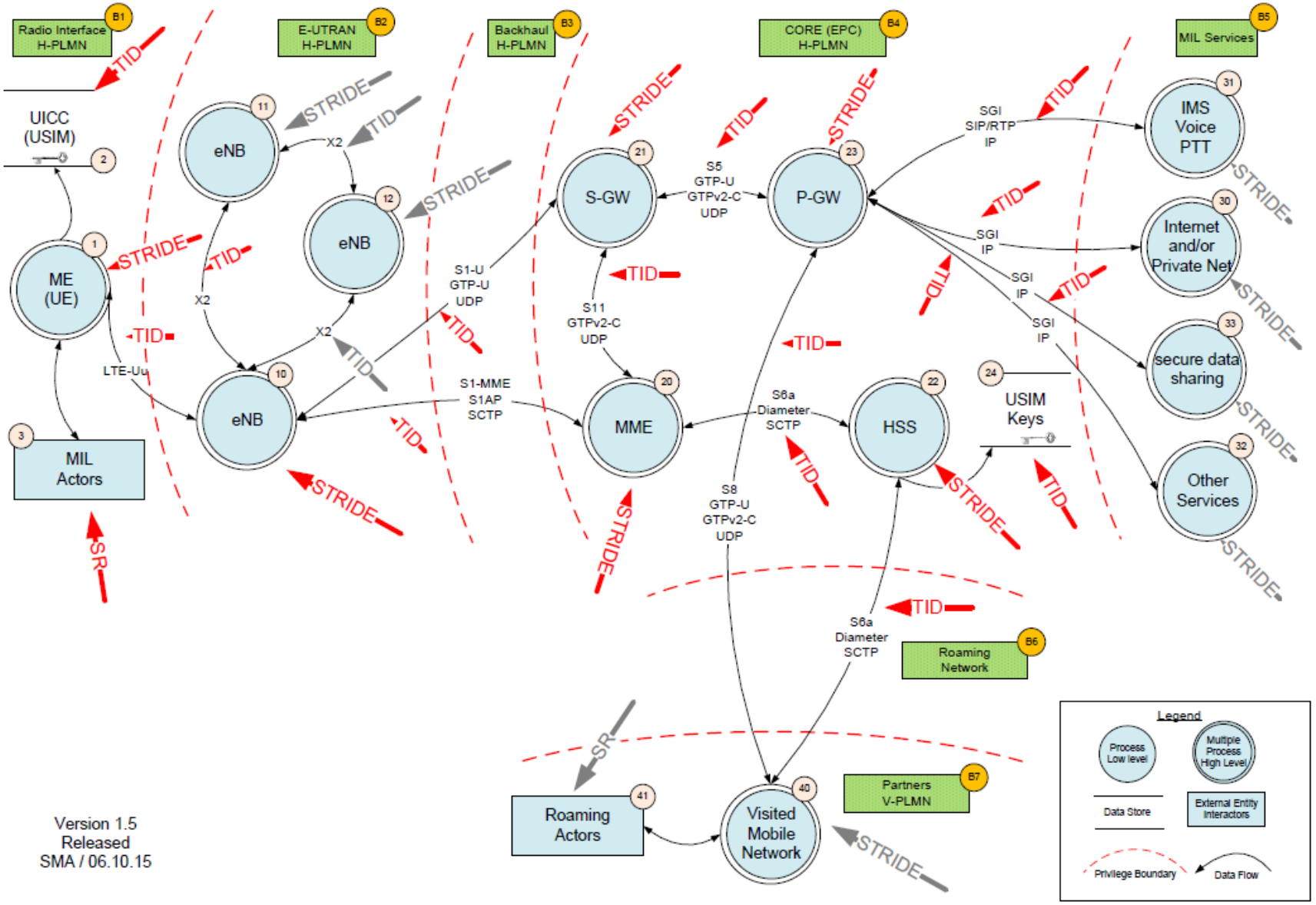
Dr. Gérôme Bovet

gerome.bovet@armasuisse.ch

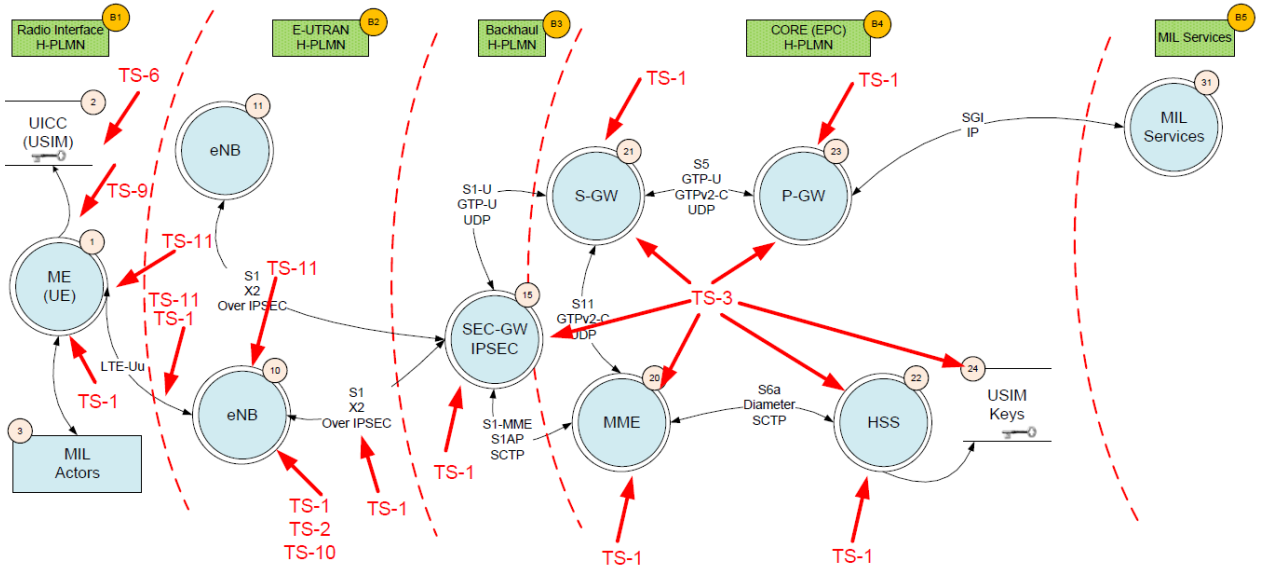
STRIDE Ansatz

- **S**poofing: Täuschungsmethoden zur Verschleierung der eigenen Identität oder Übernahme einer fremden Identität.
- **T**ampering: Absichtliche Änderung von Produkten in einer Weise, die sie schädlich machen würde.
- **R**epudation: Vergangene Aktionen zu widerrufen, kein Nachweis für die Integrität und Herkunft der Daten.
- **I**nformation disclosure: Offenlegung der Daten.
- **D**enial of Service: Ein Denial-of-Service wird typischerweise dadurch erreicht, dass die Zielmaschine oder -ressource mit überflüssigen Anforderungen überflutet wird, um Systeme zu überlasten und zu verhindern, dass einige oder alle legitimen Anforderungen erfüllt werden.
- **E**levation of privilege: Ausnutzung eines Computerbugs bzw. eines Konstruktions- oder Konfigurationsfehlers mit dem Ziel, einem Benutzer oder einer Anwendung Zugang zu Ressourcen zu verschaffen, deren Nutzung mit eingeschränkten Rechten nicht möglich ist.

Angriffsvektoren



Gefahren

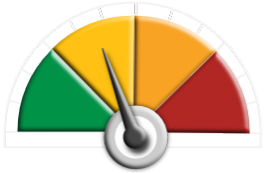


TS1	TS2	TS3	TS4	TS5	TS6
Jamming	Kompromittierter eNodeB	Kompromittierter EPC	Kompromittierter Roaming-Partner	Kompromittierte Lieferkette	Kompromittierter UE

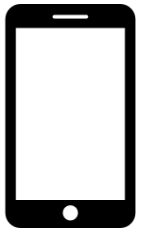
TS7	TS8	TS9	TS10	TS11	TS12
Feindselige Handlungen	Spionage/Belauschen	Verlust und/oder Diebstahl von UE	Verlust und/oder Diebstahl von eNodeB	Rogue eNodeB / IMSI catcher	Verlust und/oder Diebstahl von EPC

Massnahmen

Architecture & Governance | Continuous risk assessment | Back-end & Operations | IP Transmission | Broadcast Stations | Terminals





- RSC1-Bereitstellung von IPsec VPN Tunnels mit PKI
- RSC3-Risikobewertungsaktivitäten während der Beschaffung
- RSC4-Risikobewertungsaktivitäten vor der Bereitstellung
- RSC5-Risikobewertungsaktivitäten während dem Betrieb

- RSC6-Überwachung und Sicherheit Operation Center
- RSC12-Credentials-Bereitstellung
- RSC15-Erstellen von Sicherheitsverfahren

- RSC2-Core Network Schutz
- RSC8-Schutz der Kommunikation mit externen Netzen
- RSC14-LTE-Komponenten Härtung

- RSC7-Störsender Erkennung
- RSC11-eNodeB Schutz

- RSC9-USIM-Schutz
- RSC10-UE Härtung
- RSC13-Gesicherte Anwendungen

Massnahmen

Minderung	Aufwand/Kosten	Umsetzbarkeit
RSC1-Bereitstellung von IPsec VPN Tunnels mit PKI	$	
RSC2-Core Network Schutz	$$	
RSC3-Risikobewertungsaktivitäten während der Beschaffung	$	
RSC4-Risikobewertungsaktivitäten vor der Bereitstellung	$$	
RSC5-Risikobewertungsaktivitäten während dem Betrieb	$	
RSC6-Überwachung und Sicherheit Operation Center	$$$	
RSC7-Störsender Erkennung	$$$	
RSC8-Schutz der Kommunikation mit externen Netzen	$	
RSC9-USIM-Schutz	$$	
RSC10-UE Härtung	$	
RSC11-eNodeB Schutz	$$	
RSC12-Credentials-Bereitstellung	$$	
RSC13-Gesicherte Anwendungen	$$	
RSC14-LTE-Komponenten Härtung	$	
RSC15-Erstellen von Sicherheitsverfahren	$	

Umsetzung der Massnahmen

TS1	TS2	TS3	TS4	TS5	TS6
Jamming	Kompromittierter eNodeB	Kompromittierter EPC	Kompromittierter Roaming-Partner	Kompromittierte Lieferkette	Kompromittierter UE

TS7	TS8	TS9	TS10	TS11	TS12
Feindselige Handlungen	Spionage /Belauschen	Verlust und/oder Diebstahl von UE	Verlust und/oder Diebstahl von eNodeB	Rogue eNodeB / IMSI catcher	Verlust und/oder Diebstahl von EPC

Die Luftschnittstelle wird immer die grösste Gefahr darstellen.