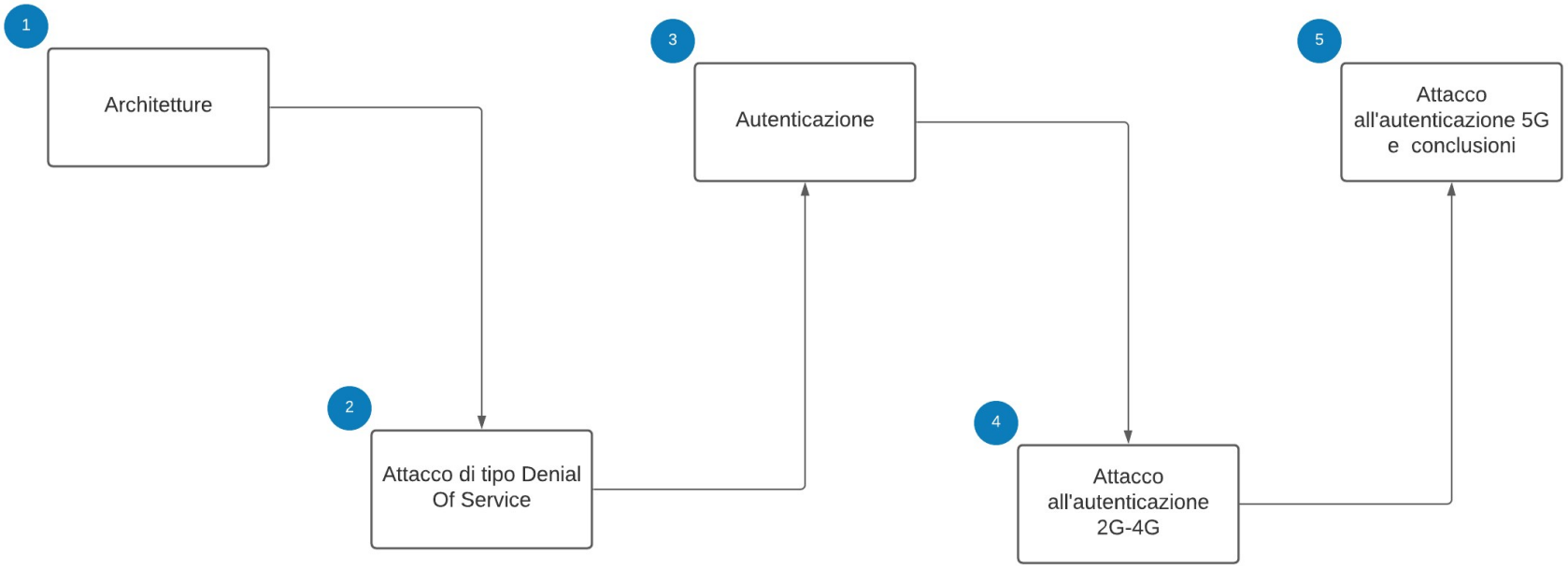
ATTACCO DI TIPO DENIAL OF SERVICE ALLE RETI CELLULARI

Laureando: Stefano Leggio
Relatore: Prof. Mauro Migliardi
Data di laurea: 20/09/2021

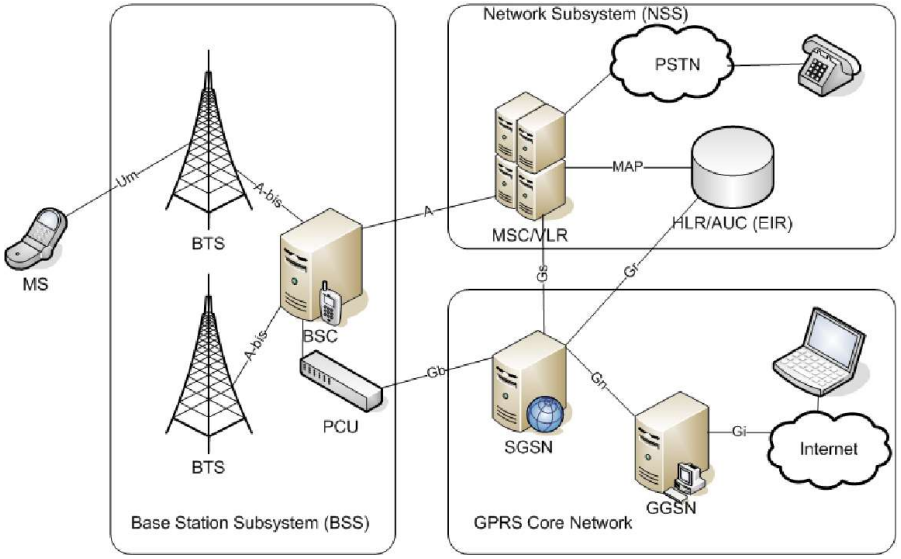
Università degli Studi di Padova
Dipartimento di Ingegneria dell'Informazione

Scopo della tesi

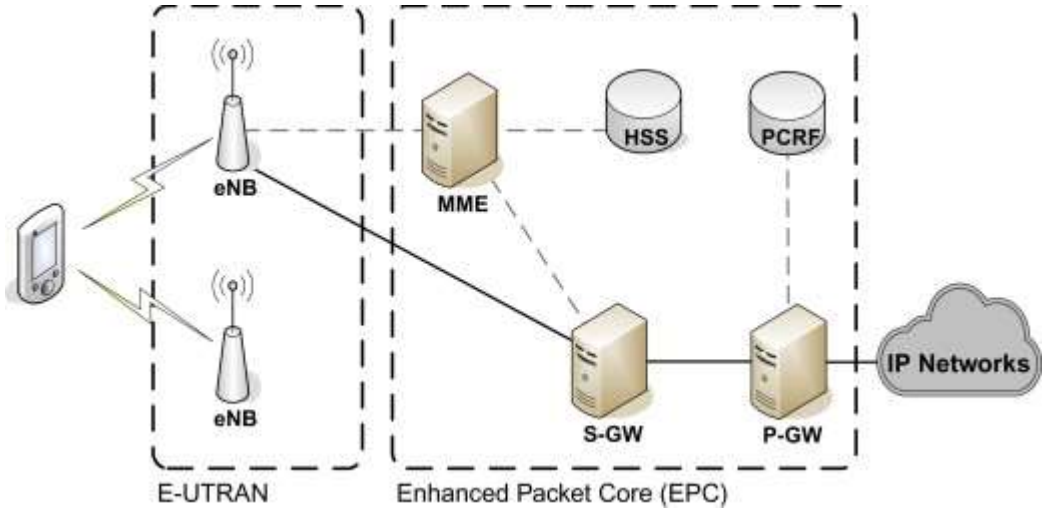
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE



Architetture 2G-4G

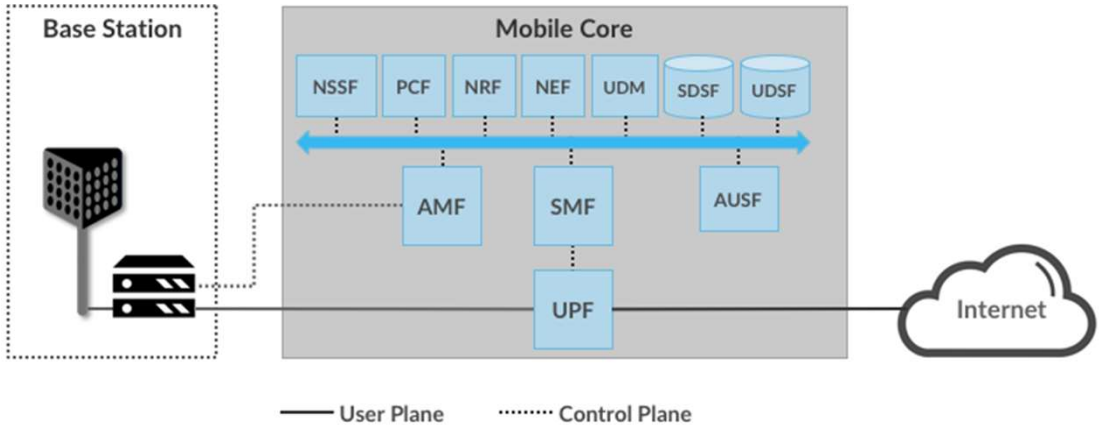


Schema architettura UMTS (3G)

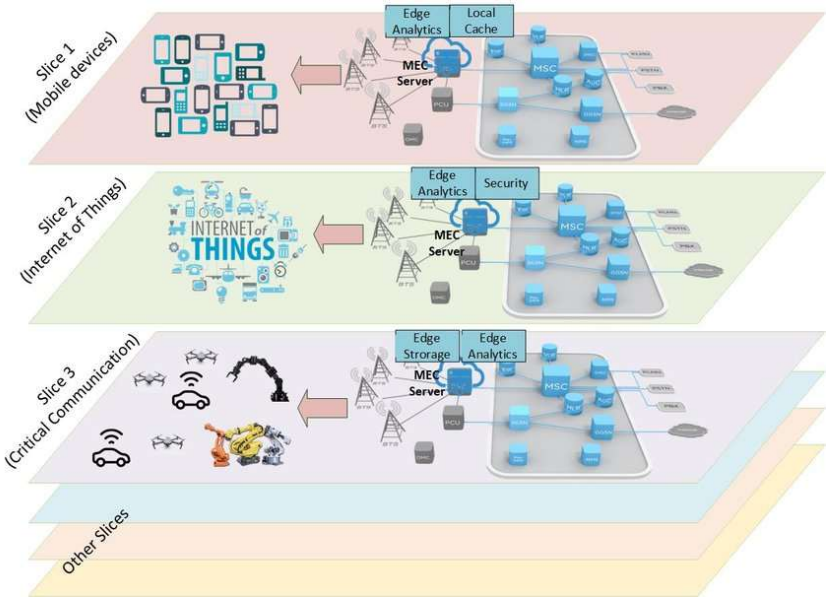


Schema architettura LTE (4G)

Architettura 5G



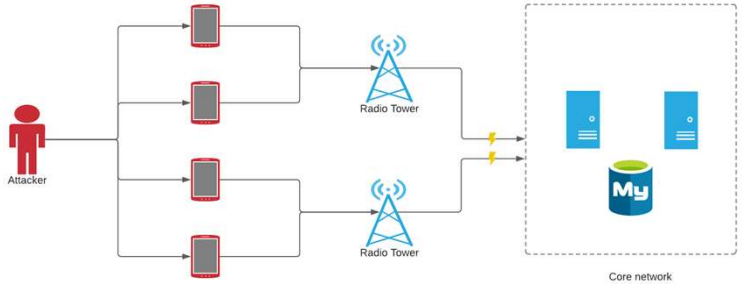
Schema architettura 5G



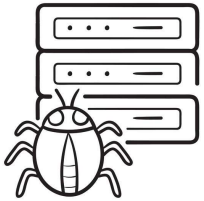
Network slicing

Attacco di tipo Denial Of Service

Radio jamming



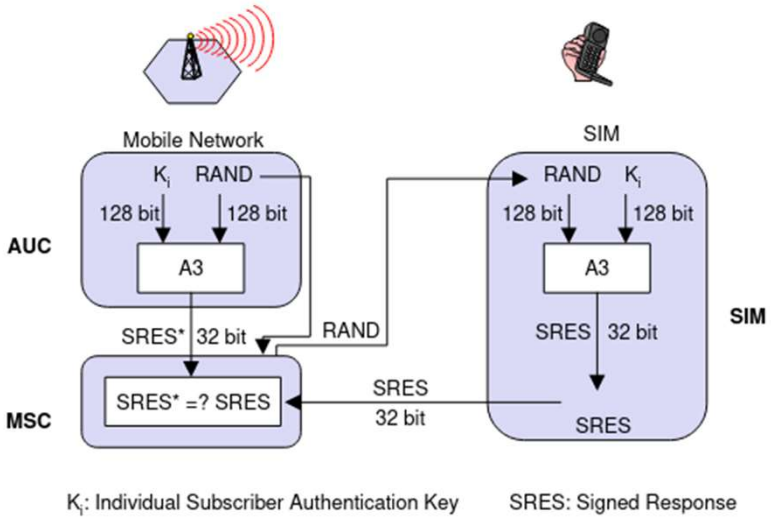
Botnet



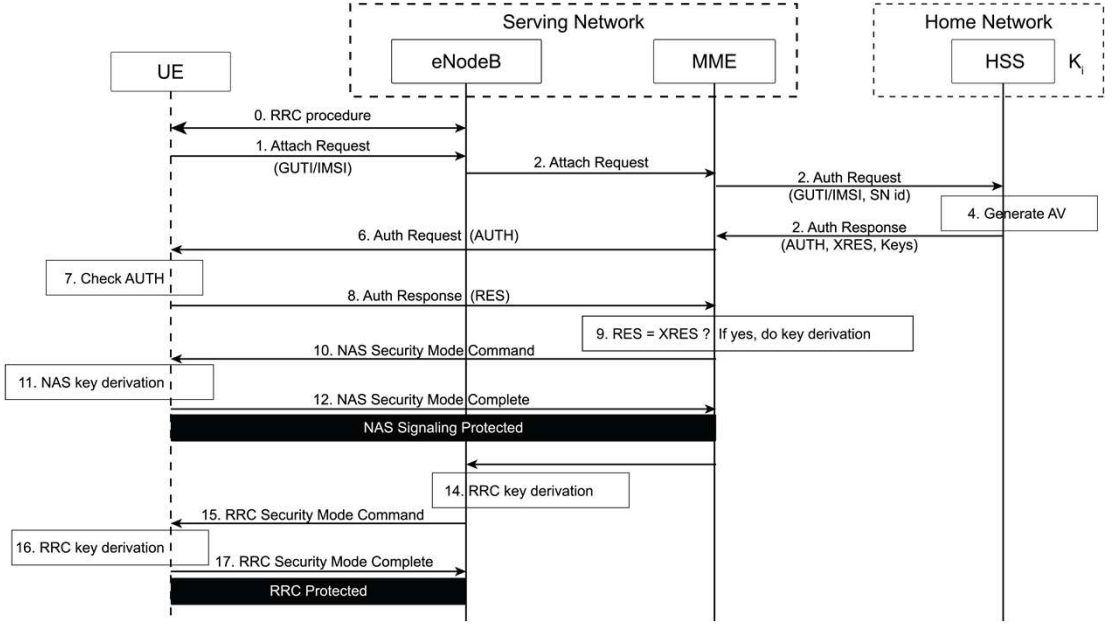
Classiche vulnerabilità

Autenticazione

Autenticazione 2G-4G

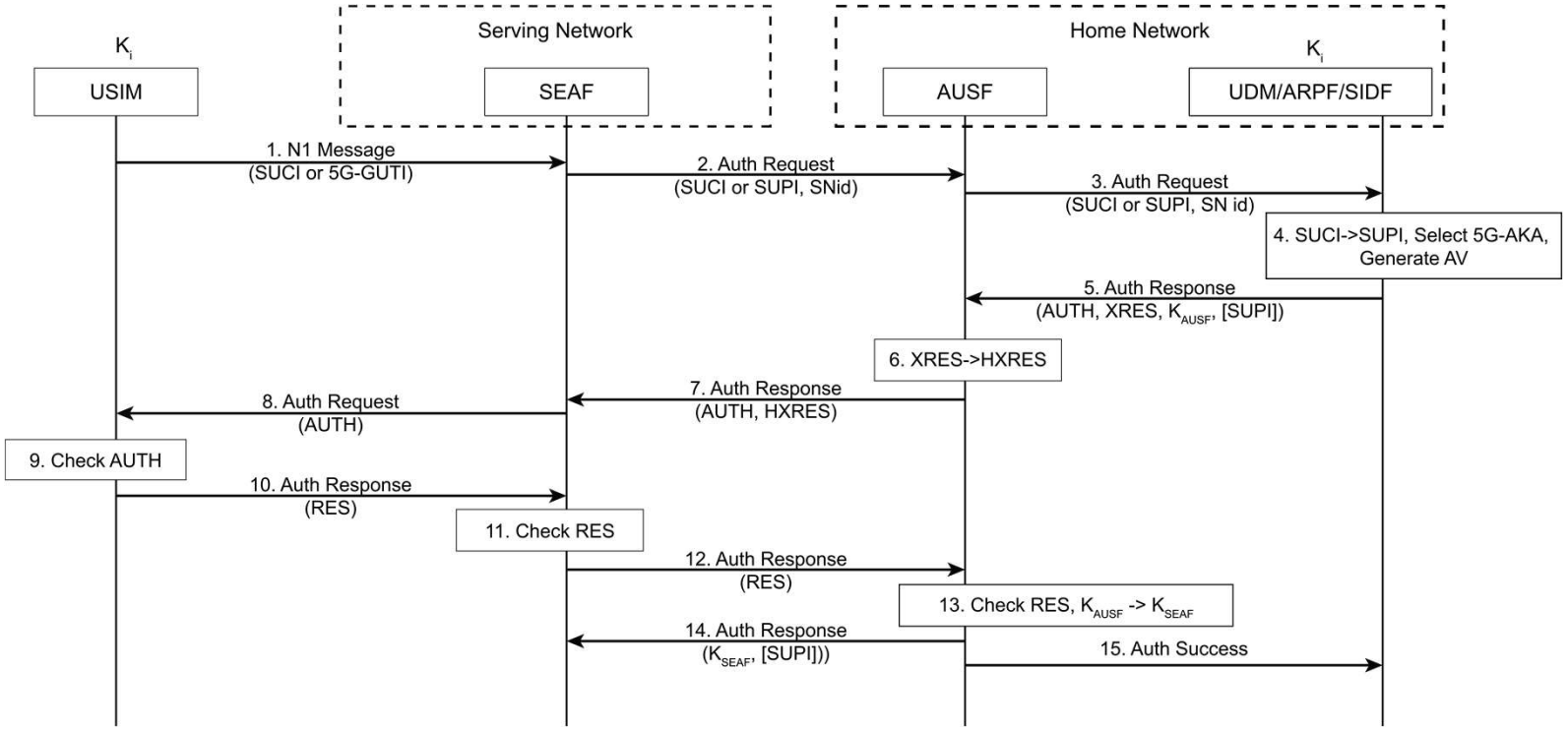


Schema autenticazione 2G



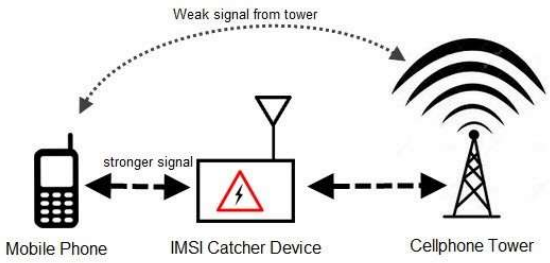
Schema autenticazione 3G e 4G

Autenticazione 5G

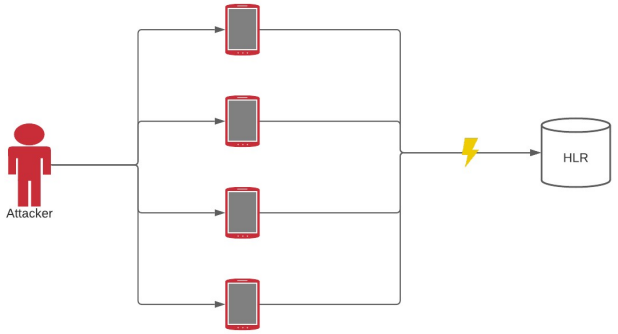


Schema autenticazione 5G

Attacco all'autenticazione 2G-4G



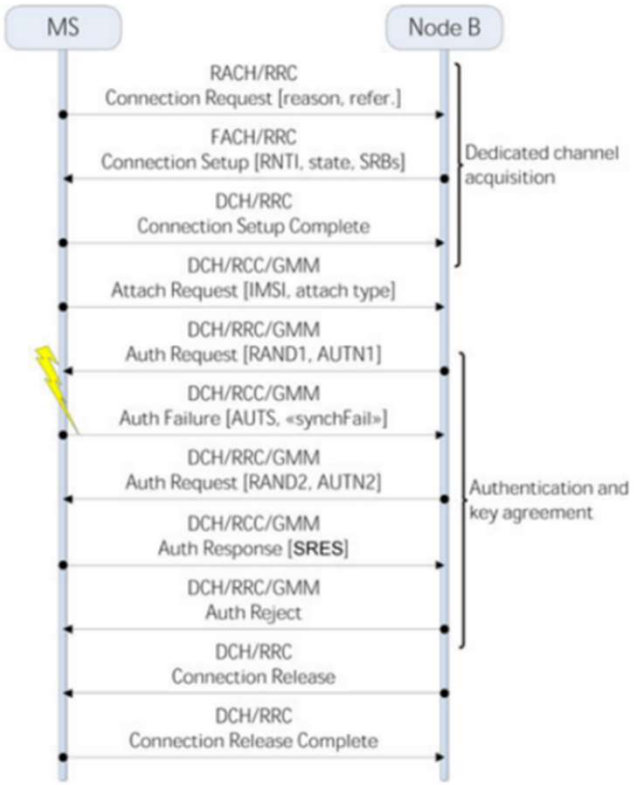
Raccolta IMSI



Attacco *botnet* in 2G/3G

Un attacco *botnet* al sistema di autenticazione permette di ottenere una degradazione delle prestazioni della HLR di oltre il 90% utilizzando più di 11k dispositivi infettati.

Attacco all'autenticazione 2G-4G



Air interface nello UMTS

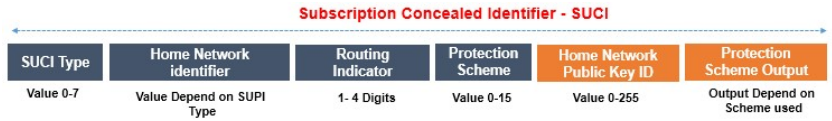
Attacco SIM-LESS

Nelle reti UMTS la capacità più stringente è nel canale FACH con 28 TPS.
Quindi bastano 446 dispositivi per effettuare una degradazione del sistema.

Attacco alle reti 5G e conclusioni

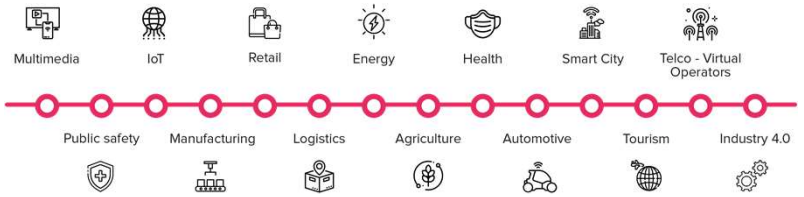
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Vantaggi
- IMSI criptato: SUCI
- SDN per il monitoraggio della rete



Composizione SUCI

Svantaggi
- Retrocompatibilità
- Autenticazione consuma più risorse
- TPS maggiori nei canali di comunicazione
- Più dispositivi collegati (IOT massivo)



Servizi nel 5G


Grazie per l’attenzione
UNIVERSITÀ DEGLI STUDI DI PADOVA
DIPARTIMENTO DI INGEGNERIA DELL’INFORMAZIONE