



UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII

Dipartimento di Ingegneria
dell'Informazione



unIMC

5G e Security

Alessandro BETTI

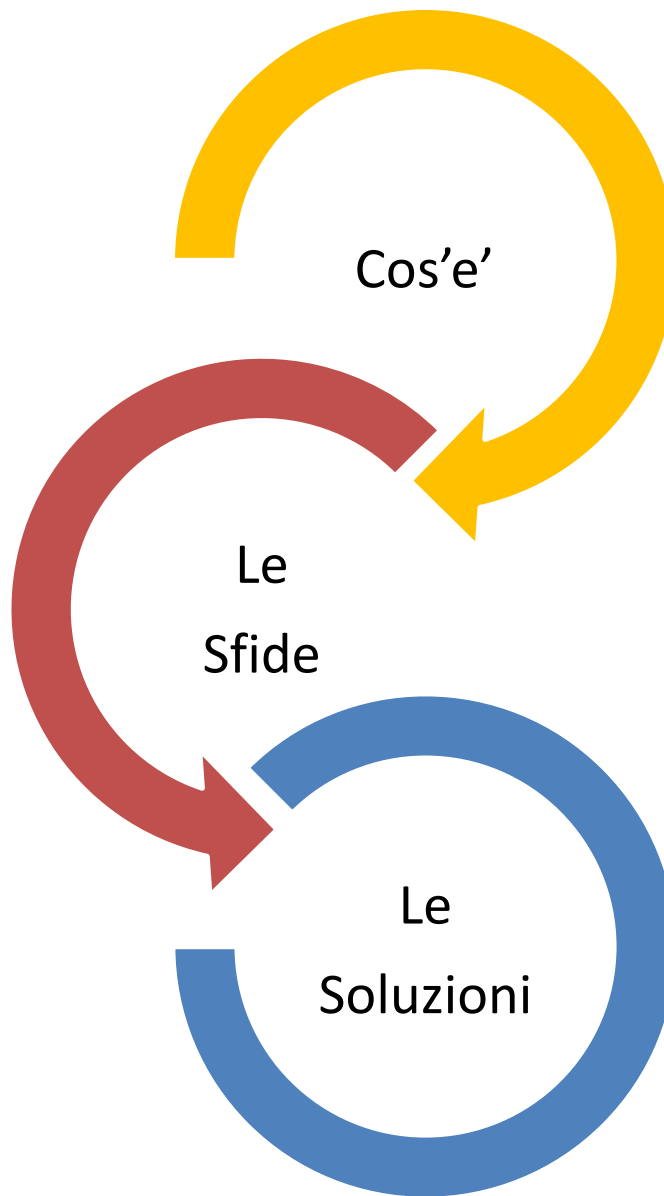
<https://www.linkedin.com/in/alessandrobetti/>
bettiale@gmail.com

Martedì 19 Luglio 2022



Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Agenda



Le promesse del 5G



mMTC

Low power
1 Million/km²

Smart cities
Smart metering
Smart agriculture



eMBB

10/20 Gbps peak rate
4ms one way

Social media
On line gaming
4K streaming
AR\VR

uRLCC

1 ms one way
99.999%

Industrial sectors
Smart manufacturing
Healthcare

Transport
Logistic
Drones

Le sfide del 5G



IT transformation

Topologia

Funzioni

Attori\ruoli

Device

Resilienza

VNF\CNF+PNF
Aumento vendor ecosystem
OpenSource

Centralised
Edge
Private Network
Private Cloud vs Public Cloud

CUPS native
Slicing\Virtual network
Orchestration
SBA (Service Based Architecture)
CI\CD

Incremento MVNOs (ESP, Full)
Roaming (es PNRR)
RAN Sharing & Broker

Ampia diffusione
Costo ridotto\bassa sicurezza

Applicazioni\servizi critici
(utilities\sanità\difesa)

**SUPERFICIE
DI ATTACCO
AMPLIATA**



5G

Autenticazione mutua fra entità nella SBA e cifratura (IPSEC, TLS 1.2\1.3 Oauth 2.0)

Access authentican (Primary\secondary 3PP)
Estensione a EAP (piu' tipi di credenziali e metodi di auth Internet based)



IT transformation

Security basata su approccio olistico automatizzato considerando ambiente non sicuro

Topologia

(SEPP) Security Edge Protection Proxy per la segnalazione, con scambio certificati interoperatore interfaccia N32 per user data



Funzioni

IPUPS (InterPLMN UPS Security on GTP-U) (Edge o Roaming)

Attori\ruoli

Essendo dual mode core anche per 4G, introduzione di GTP FW e Diameter FW per GSMA cat 1\2\3

Device

Gestione della Subscriber identity migliorata (es uso mandatorio identità temporanee anziché permanenti per evitare eavesdropper o Stingray)

Resilienza

Normativa nazionale (PNSC, Golden Power, Resilienza) che induce revisione continua governance\processi in termini di richieste\frequenza\verifiche sistemi\analisi criticità sistemi\ accessi\analisi obsolescenze\PSIRT\Logging

asset inventory costantemente aggiornati per valido ICT Risk Management

**SUPERFICIE
DI
ATTACCO
RIDOTTA**

Main references



<http://www.3gpp.org>

<https://www.ericsson.com>

<https://www.fortinet.com>

<https://www.enisa.europa.eu>

<https://www.agv.gov.it>



GRAZIE