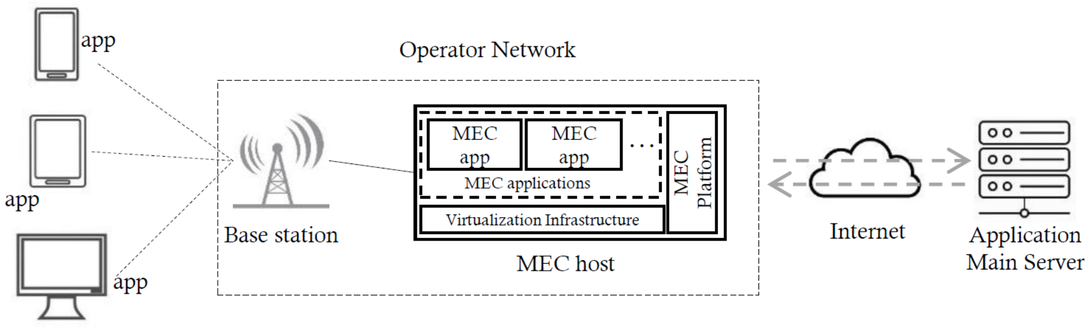
HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI
MATEMAATTIS-LUONNONTIETEELLINEN TIEDEKUNTA
MATEMATISK-NATURVETENSKAPLIGA FAKULTETEN
FACULTY OF SCIENCE

Gizem Akman
Valtteri Niemi
Department of Computer Science,
University of Helsinki
Philip Ginzboorg
Huawei, Finland

Privacy for Users of Multi-Access Edge Computing (MEC) Applications

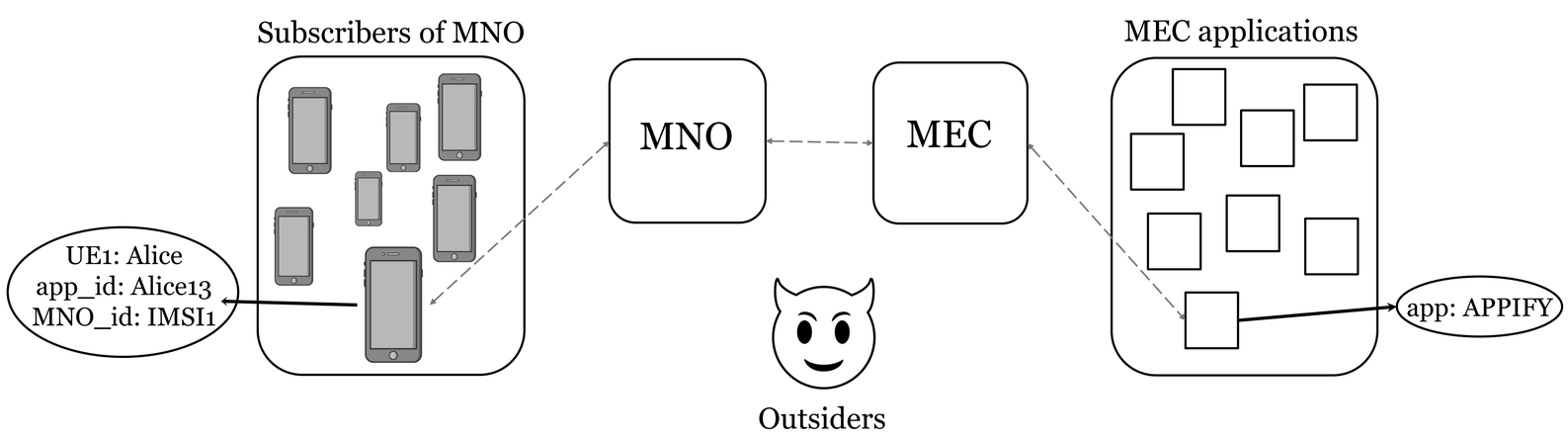


MEC is one of the emerging key technologies in 5G Mobile Networks, providing reduced end-to-end latency for applications and reduced load in the transport network.

Scenario

Alice is a subscriber of a Mobile Network Operator, MNO. Alice wants to use a MEC application, which is called APPIFY.

- In order to use APPIFY, the messages of Alice should go through the network of MNO and the MEC host.
- Even though the traffic between the parties are encrypted, the MNO and the MEC host can see the message flow between Alice and APPIFY.
- Still, Alice wants to communicate with APPIFY without revealing the identity of APPIFY and the content of the messages to MNO.
- Alice also wants to be anonymous towards MEC host.



Dependent Parties

Dependent parties share information which is not strictly needed for providing the service. This may happen, for example, when the parties are part of the same company. There are five possible combinations of dependent parties in our scenario.
1) MNO, MEC, and APPIFY are all independent.
2) MNO and MEC are dependent.
3) MEC and APPIFY are dependent.
4) MNO and APPIFY are dependent.
5) MNO, MEC, and APPIFY are all dependent.

Adversary Models

MNO, MEC, and APPIFY : Honest-but-Curious + Passive Dolev-Yao

Outsiders : Dolev-Yao

Other UEs : Malicious

Alice : not an adversary in this scenario

Privacy Requirements

R1-MNO-I	MNO should not learn that Alice13 is the identifier of Alice for APPIFY.
R2-MNO-D	MNO should not learn what content Alice sends to and receives from APPIFY.
R3-MNO-D	MNO should not learn which APPIFY Alice is using.
R4-MNO-U	MNO should not be able to distinguish whether two messages go to the same MEC application.
R5-MNO-U	MNO should not be able to distinguish whether two messages are related to the same user identifier for MEC application.
R6-MEC-I	MEC should not learn that identities Alice, Alice13, or IMSI1 are relevant to the messages.
R7-MEC-D	MEC should not learn the content that Alice sends to and receives from APPIFY.
R8-MEC-U	MEC should not be able to distinguish whether two messages are related to the same user, same IMSI, or same identifier of MEC application.
R9-APP-I	APPIFY should not learn that Alice or IMSI1 is related to Alice13.
R10-APP-D	APPIFY should not learn anything related to Alice, if Alice does not provide such information.
R11-APP-U	APPIFY should not distinguish whether two messages are coming from the same device.
R12-APP-U	APPIFY should not distinguish whether two messages are related to the same IMSI.
R13-OUT-I	Outsiders should not learn anything related to identities.
R14-OUT-D	Outsiders should not learn which MEC application Alice is using.
R15-OUT-D	Outsiders should not learn the content of what Alice is sending and receiving.
R16-OUT-U	Outsiders should not be able to distinguish whether two UEs use the same MEC application.
R17-OUT-U	Outsiders should not be able to distinguish whether two messages are related to the same MEC application.

Privacy notions

Identity Confidentiality (I) – user identity of a user to whom a services is delivered cannot be eavesdropped on the radio access link [1].

Data Confidentiality (D) – protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft [2].

Unlinkability (U) – unlinkability of two or more items of interest from an attacker's perspective means that within the system, the attacker cannot distinguish whether these items are related or not [3].

REFERENCES

1) 3GPP TS33.102 V16.0.0.: 3G Security; Security architecture. Technical Specification, (2020).
2) University of Delaware, Secure UD: Managing data confidentiality, {https://www1.udel.edu/security/data/confidentiality.html}. Last accessed: 28 Jul 2020.
3) Paverd, A.J., Martin, A., Brown, I.: Modelling and Automatically Analyzing Privacy Properties for Honest-but-Curious Adversaries. Technical Report (2014).
4) Image : https://www.vecteezy.com/vector-art/550874-devil-face