Radboud University

Advanced Network Security

Lecture 6: Enhanced Subscriber Privacy

Special Guest: David Rupprecht, Katharina Kohls

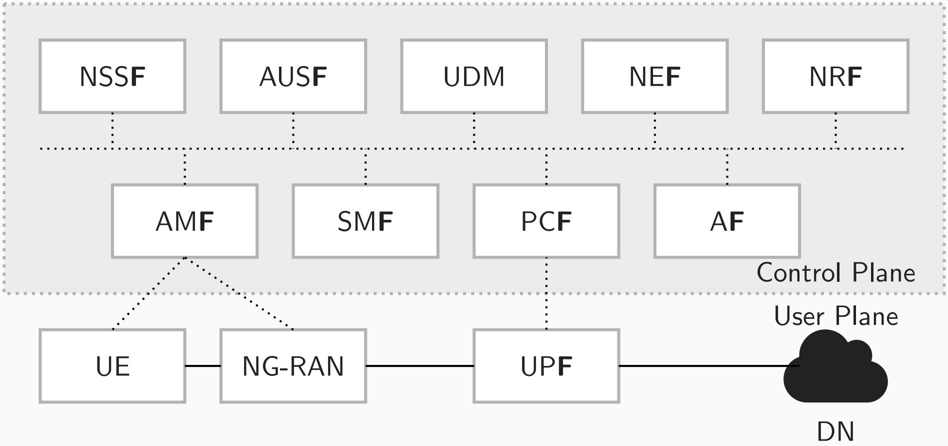
October 13, 2022

Open University Nijmegen
Radboud University Nijmegen

Recap

Service-Based Architecture	Unified Access-agnostic Authentication	5GC-EPS Interworking Security	RAN Security DU-CU Split
User Plane Integrity Protection	Primary Authentication	Visibility Configurability	Interconnection Security SEPP
Enhanced Subscriber Privacy	Increased Home Control	Secondary Authencication	Initial NAS Message Protection

Service-Based Architecture



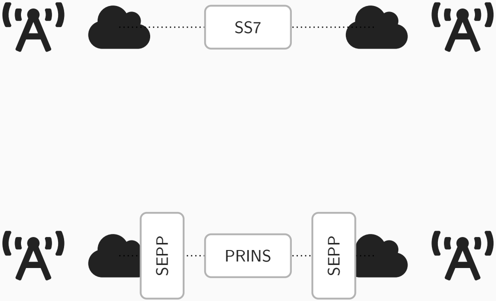
Mandatory Integrity Protection

- 4G: No integrity protection for user plane data
- User data redirection (L4), Full Impersonation (skipped)
- 5G: Mandatory to support
- Optional to use by operator

What are challenges of mandatory integrity protection?

- Overhead
- Deployment

Interconnection Security SEPP



Before 5G

- SS7 network (70s) based on trust
- Many attacks on user tracking, eavesdropping

5G Standalone

- Security Edge Protection Proxy (SEPP)
- HTTPS and PRotocol for N32 INterconnect Security (PRINS)

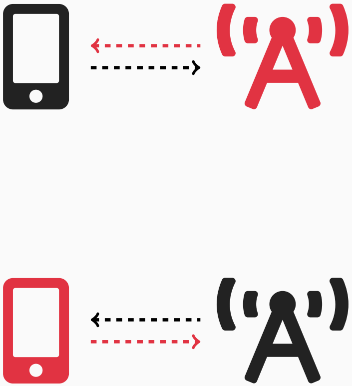
5G Improvements

Service-Based Architecture	Unified Access-agnostic Authentication	5GC-EPS Interworking Security	RAN Security DU-CU Split
User Plane Integrity Protection	Primary Authentication	Visibility Configurability	Interconnection Security SEPP
Enhanced Subscriber Privacy	Increased Home Control	Secondary Authencication	Initial NAS Message Protection

Authentication $\leftrightarrow$

- UE and eNodeB authenticate each other
- Can protect against Man-in-the-Middle, replay, spoofing attacks

Why are we looking at this? We need identifiers for mutual authentication!

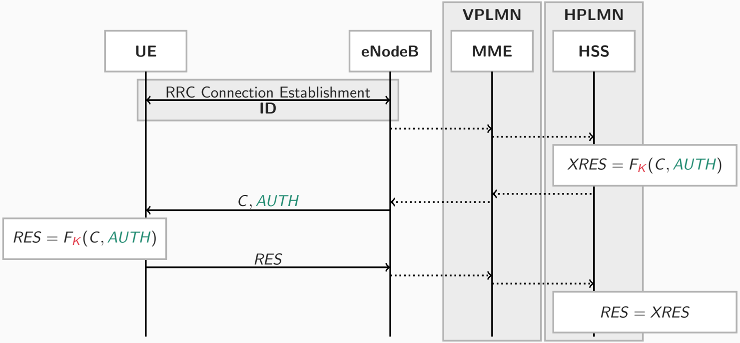


Mutual Authentication in LTE:

- LTE uses a challenge-response protocol to establish **mutual authentication** between the UE and the network
- The protocol uses symmetric key cryptography
- The UE has its secret K on the SIM card
- The operator stores their secrets K in the core network (HSS)

Authentication and Key Agreement AKA:

- Before the AKA, the RRC Connection Establishment takes place
- (Remember the Identity Mapping attack of last week, RNTIs, . . .)
- In this process, the UE sends its ID towards the network
- The ID is used to check the correct individual information


VPLMN
HPLMN
UE
eNodeB
MME
HSS
RRC Connection Establishment
ID
$XRES = F_K(C, AUTH)$
$C, AUTH$
$RES = F_K(C, AUTH)$
RES
$RES = XRES$

Authentication and Key Agreement

(1) After connection was established, network sends the challenge C and authentication token $AUTH$

(2) Network generates individual $XRES$

(3) UE uses secret K to generate RES

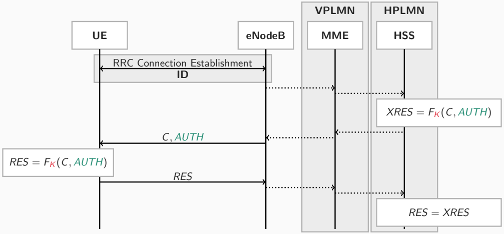
(4) Send RES towards network, where it's compared to $XRES$

Important:

- The authentication token $AUTH$ authenticates the network towards the UE
- $RES = XRES$ authenticates the UE towards the network
- The eNodeB only does the communication. All important computations are done in the *core network*.

AKA Core Components

- Challenge C: Like a nonce
- Authentication Token AUTH: ID-specific
  - Sequence number, receives updates whenever used
  - In sync between HSS and UE
  - Authenticates network to UE
- Cryptographic function F: Generate tokens RES and $XRES$
- Secret K: Symmetric key



Enhanced Subscriber Privacy

Permanent and Temporary

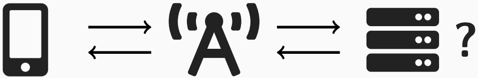
- Unique identifier on the SIM card
- Because AKA uses a shared symmetric key, it can only happen after user identification
- Sending the IMSI/SUPI in plaintext means a user can be identified and tracked ☹
- **To avoid this, temporary identifiers are used!**

	4G	5G
Permanent	IMSI	SUPI
Temporary	TMSI	GUTI

First Contact

It's not always possible to use the temporary identifiers.

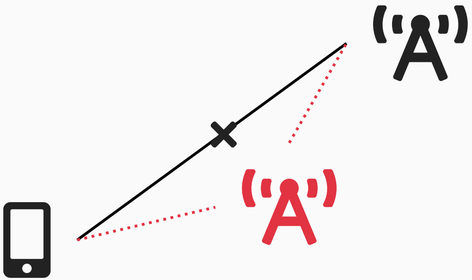
When does a temporary identifier not work?



Contacting the Network

- Temporary identifiers need to be assigned
- When the user visits for the first time, there is no TMSI/GUTI for the user
- Special case: IMSI/SUPI cannot be derived from the TMSI/GUTI

4G IMSI Catchers



Man-in-the-Middle

(1) UE connects to legitimate eNodeB

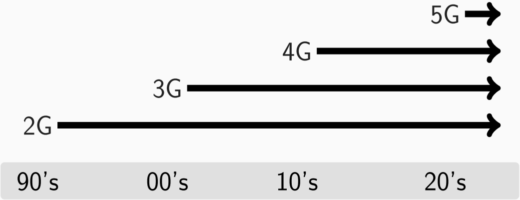
(2) Attacker places a fake base station

(3) Stronger signal makes user connect to fake bts

(4) **Attacker can force the user to share permanent identifiers!**

Backward Compatibility

- 2G/3G/4G are vulnerable to IMSI catchers
- Main reason: Backward compatibility
- 5G solves the problem at the cost of backward compatibility



How do they do it?

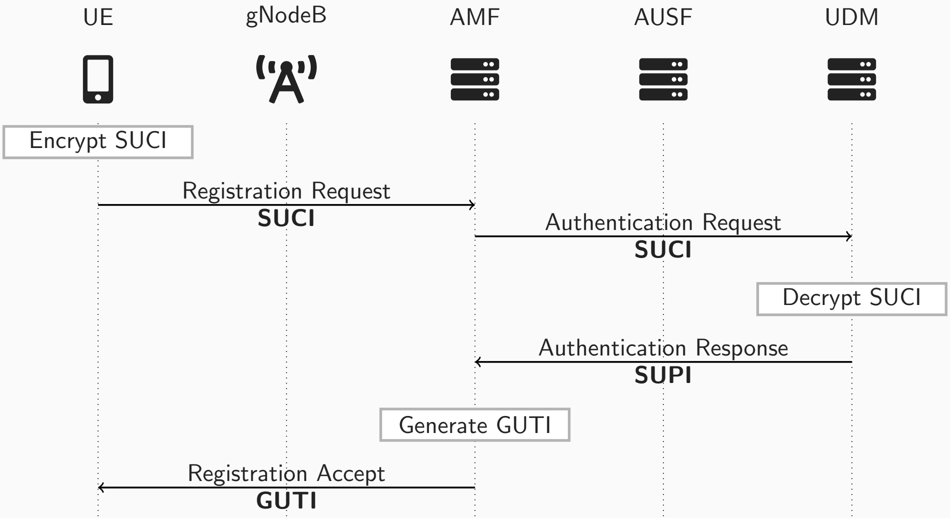
No Plaintext Transmission of Permanent Identifiers

Subscription Concealed Identifier (SUCI)

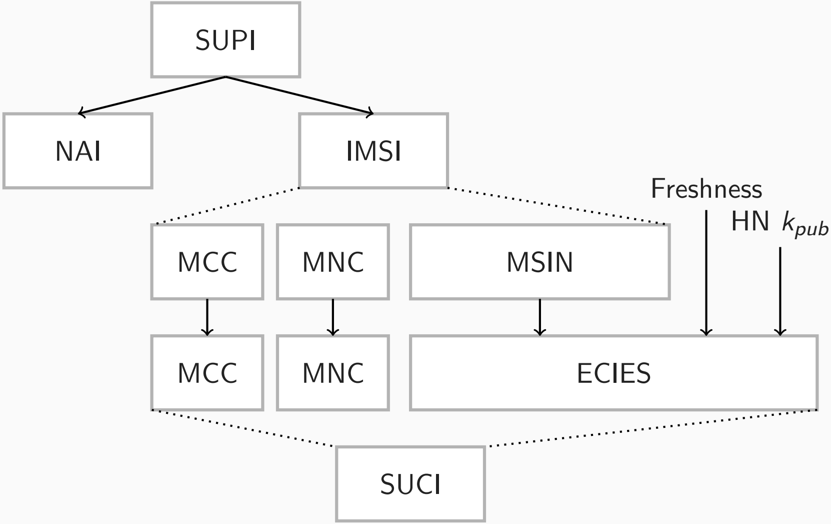
- Whenever the SUPI is needed, a concealed version is sent instead
- Elliptic Curve Integrated Encryption Scheme (ECIES) [1]
- The SUCI is sent instead of the plaintext permanent SUPI

[1] ECIES combines a Key Encapsulation Mechanism with a Data Encapsulation Mechanism. It derives a bulk encryption key and MAC key from a common secret. It's a hybrid scheme that uses an asymmetric approach to send a symmetric key.

5G Identity Exchange



From SUPI to SUCI



From SUPI to SUCI

- The SUPI consists of
  - IMSI: Standard case we know from 4G; unique personal number
  - NAI: New 5G setting, personal address like `user@homerealm.example.net`
- IMSI has MCC and MNC as "preamble", example KPN Telecom B.V.:
  - `MCC 204`
  - `MNC 69`
- MSIN is a personal, permanent, unique number
- Needs protection, gets encrypted using a fresh input and a public key

SUCI in a PCAP Trace

registration_request_suci.pcapng

```
git clone https://github.com/P1sec/CryptoMobile.git
cd CryptoMobile
python setup.py install
```

SUPI Encryption

Packet 1

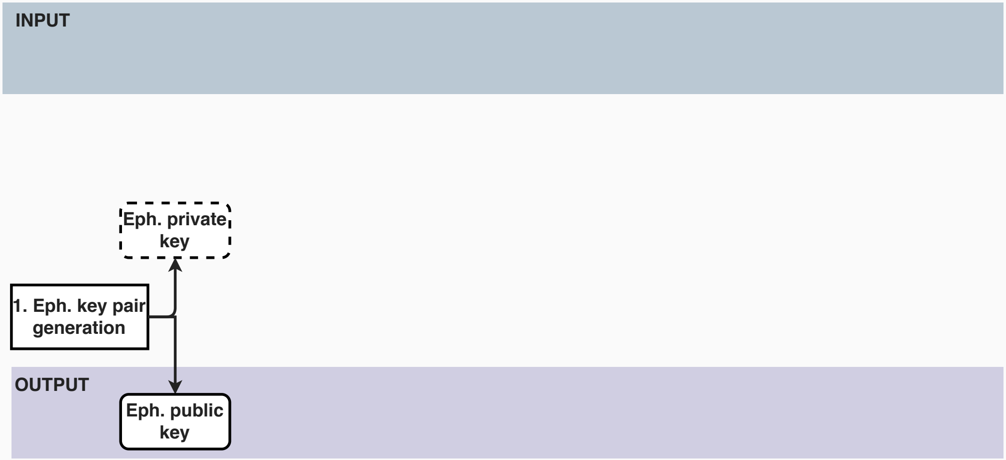
```
5GS mobile identity
    Length: 52
    0... .... = Spare: 0
    .000 .... = SUPI format: IMSI (0)
    .... 0... = Spare: 0
    .... .001 = Type of identity: SUCI (1)
    Mobile Country Code (MCC): France (208)
    Mobile Network Code (MNC): Thales communications & Security (93)
    Routing indicator: 0
    .... 0001 = Protection scheme Id: ECIES scheme profile A (1)
    Home network public key identifier: 0
    Scheme output: 7b27b315a3423f7ca10fdb77028798f86b1f58fa876cc864514a8f882d33c40431a0371c…
        ECC ephemeral public key: 7b27b315a3423f7ca10fdb77028798f86b1f58fa876cc864514a8f882d33c404
        Ciphertext: 31a0371c
        MAC tag: 0x7bdd02efd7162ba2
```

SUPI Encryption

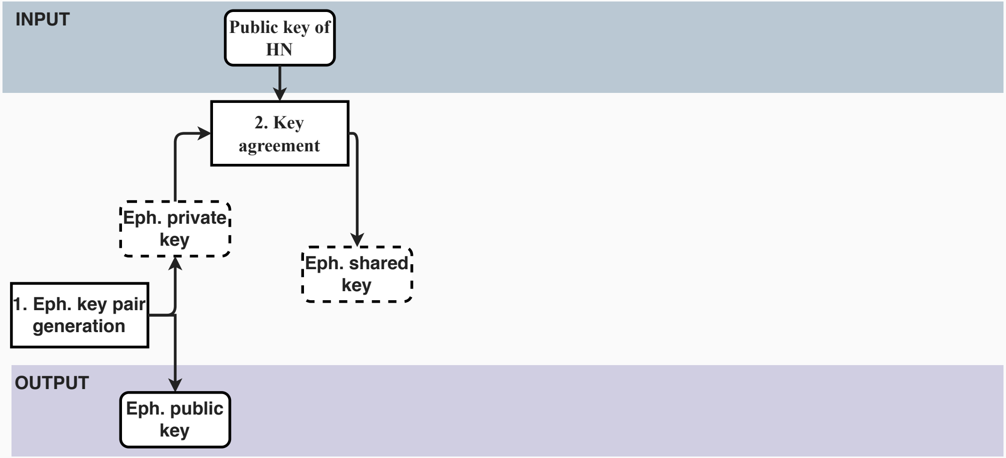
Packet 2

```
5GS mobile identity
    Length: 52
    0... .... = Spare: 0
    .000 .... = SUPI format: IMSI (0)
    .... 0... = Spare: 0
    .... .001 = Type of identity: SUCI (1)
    Mobile Country Code (MCC): France (208)
    Mobile Network Code (MNC): Thales communications & Security (93)
    Routing indicator: 0
    .... 0001 = Protection scheme Id: ECIES scheme profile A (1)
    Home network public key identifier: 0
    Scheme output: b34b34516dafed6973956d4cdd548d1e5d568bba76f29a9a0c17e62c283492392f1fd3e7…
        ECC ephemeral public key: b34b34516dafed6973956d4cdd548d1e5d568bba76f29a9a0c17e62c28349239
        Ciphertext: 2f1fd3e7
        MAC tag: 0xe158a42f076118da
```

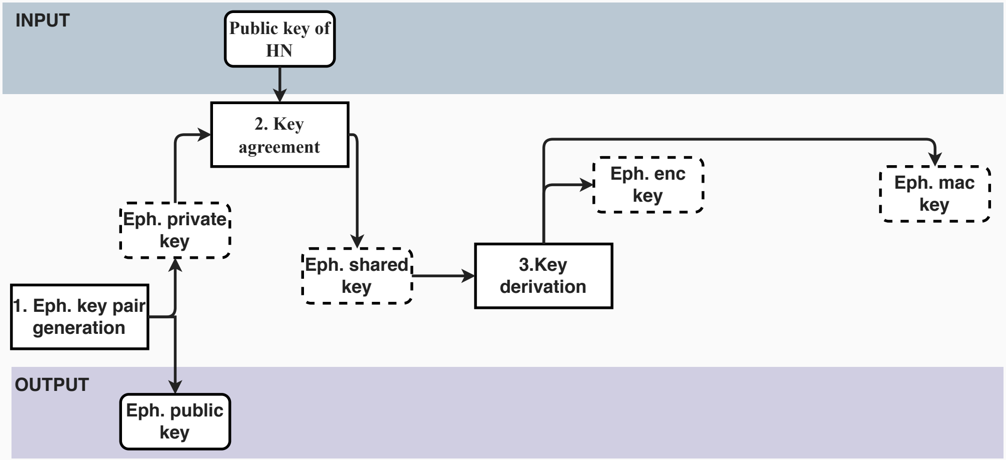
From SUPI to SUCI – Encryption — Step 1



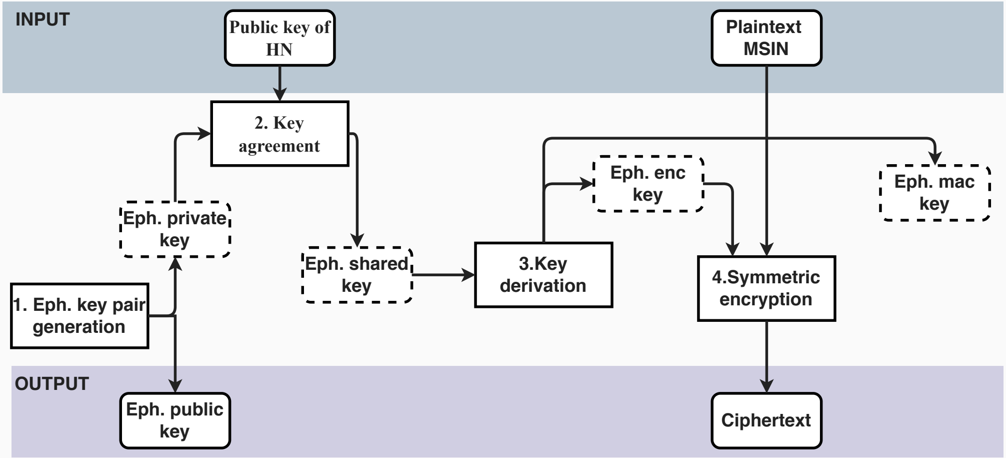
From SUPI to SUCI – Encryption — Step 2



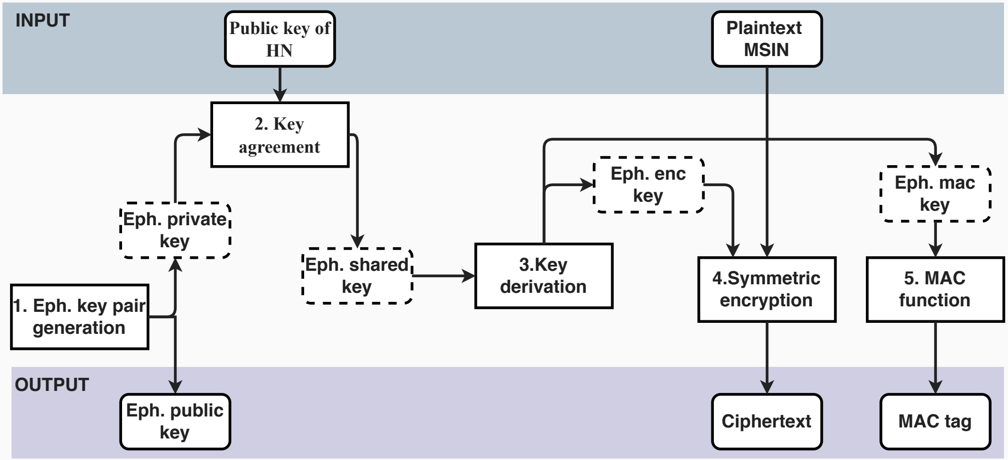
From SUPI to SUCI – Encryption — Step 3



From SUPI to SUCI – Encryption — Step 4



From SUPI to SUCI – Encryption — Step 5



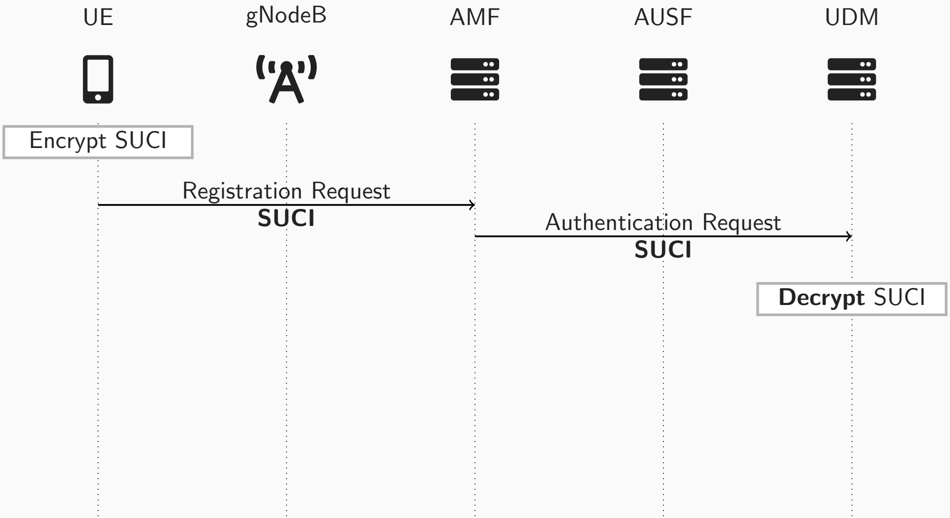
SUPI Encryption

`routing_idicator = 0, home_network_pub_key_id = 0`

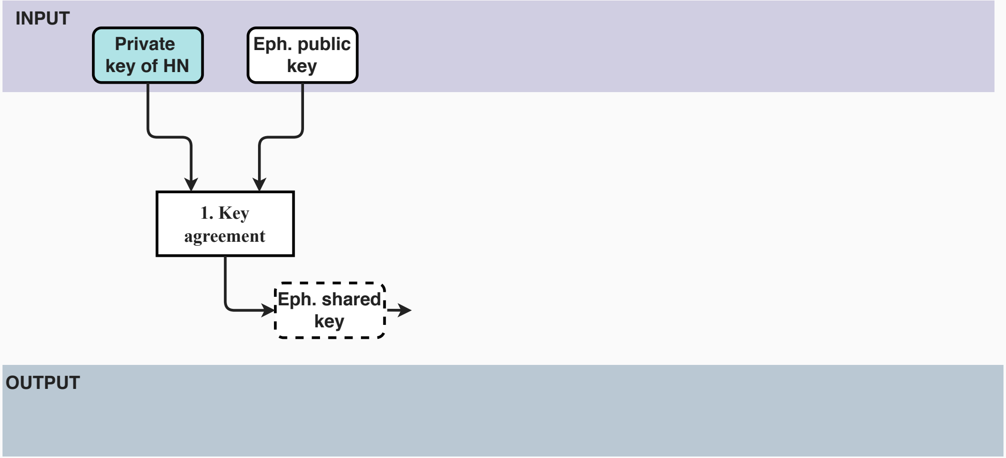
`hn_pubkey_str =`

`b'5a8d38864820197c3394b92613b20b91633cbd897119273bf8e4a6f4eec0a650'`

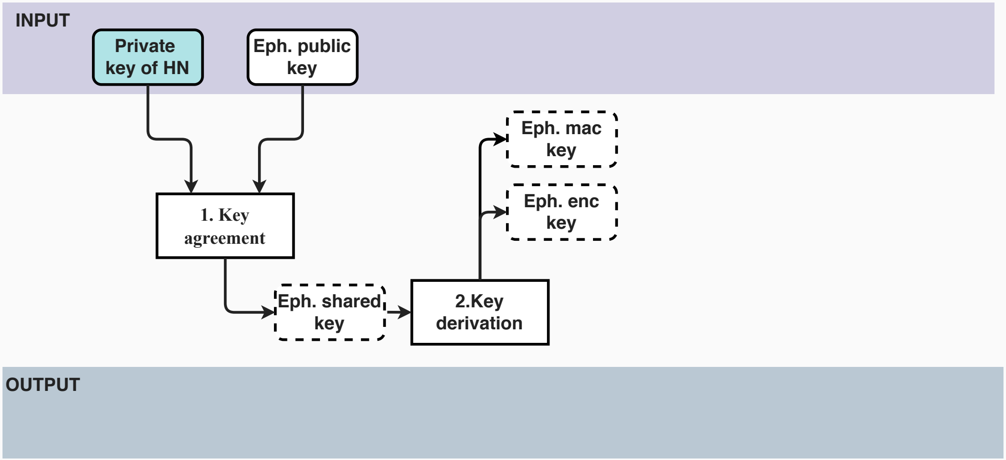
5G Identity Exchange



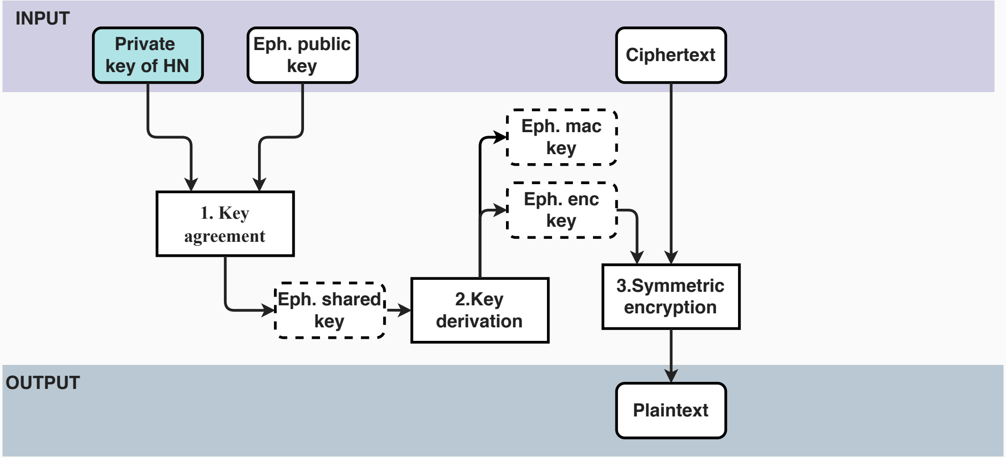
From SUCI to SUPI – Decryption — Step 1



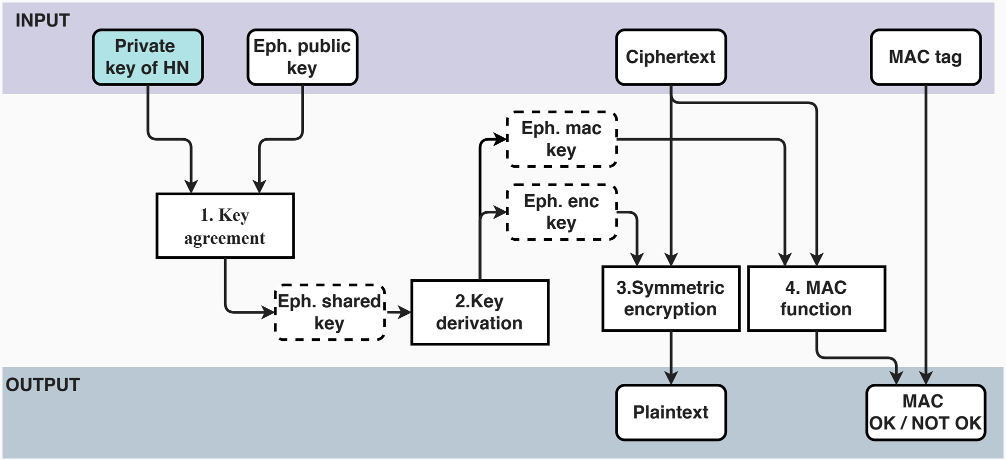
From SUCI to SUPI – Decryption — Step 2



From SUCI to SUPI – Decryption —– Step 3



From SUCI to SUPI – Decryption — Step 4



SUCI Decryption

`hn_privkey_str = b'c53c22208b61860b06c62e5406a7b330c2b577aa5558981510d128247d38bd1d'`

This Lecture

5G SUCI-Catchers: Still catching them all?

Merlin Chlosta, merlin.chlosta@rub.de, Ruhr University Bochum, Germany
David Rupprecht, david.rupprecht@rub.de, Ruhr University Bochum, Germany
Christina Pöpper, christina.poepper@nyu.edu, NYU Abu Dhabi, United Arab Emirates
Thorsten Holz, thorsten.holz@rub.de, Ruhr University Bochum, Germany

ABSTRACT

In mobile networks, IMSI-Catchers identify and track users simply by requesting all users' permanent identities (IMSI) in range. The 5G standard attempts to fix this issue by encrypting the permanent identifier (now *SUPI*) and transmitting the *SUCI*. Since the encrypted SUCI is re-generated with an ephemeral key for each use, an attacker can no longer derive the user's identity. However, this scheme does not prevent all tracking and linking: if the identity of a user is already known, an attacker can *probe* users for that identity.

We demonstrate a proof-of-concept 5G SUCI-Catcher attack in a 5G standalone network. Based on prior work on linkability through the Authentication and Key Agreement (AKA) procedure, we introduce an attack variant that enables practical, repeatable attacks. We capture encrypted SUCIs and use the AKA-procedure to link the encrypted identities between sessions. This answers *Is user X present now?* — a typical scenario for IMSI-Catchers. We analyze the attack's scalability, discuss real-world applicability, and possible countermeasures by network operators.

CCS CONCEPTS

• **Networks → Mobile and wireless security**.

KEYWORDS

5G Security, IMSI-Catcher, SUCI-Catcher, Fake Base Station, AKA, SUPI, SUCI, IMSI, Subscription Concealed Identifier

ACM Reference Format:
Merlin Chlosta, David Rupprecht, Christina Pöpper, and Thorsten Holz. 2021. 5G SUCI-Catchers: Still catching them all?. In *Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '21), June 28–July 2, 2021, Abu Dhabi, United Arab Emirates.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3448300.3467826

1 INTRODUCTION

Tracking prevention is an important security and privacy goal of mobile networks: only the operator should know the identity and location of users [1, 5.1.1]. In reality, however, the previous mobile network generations (2G, 3G, 4G) suffer from shortcomings in the standard that enable the tracking of users. One expectation for the 5th generation (5G) of mobile networks was to solve this issue.

The most popular and widespread radio-layer tracking technique involves *IMSI-Catchers* (sometimes called *Stingrays*), used by law enforcement agencies and others for surveillance [9, 20]. Commercial IMSI-Catchers work as a Fake Base Station, i. e., they copy the identity of the real network and actively *request* the user's permanent identity [18]. Any user within range eventually connects to the IMSI-Catcher and thus unwillingly exposes his or her identity. There are two main use cases: *i) Who is currently nearby?* The attacker records the identity of all nearby users. *ii) Is a particular individual present?* Here, the attacker checks if a known Person of Interest (PoI) is within reach of the IMSI-Catcher.

5G standalone (SA) deployments promise a countermeasure against IMSI-Catchers: the Subscription Permanent Identifier (SUPI) (equivalent to the International Mobile Subscriber Identity (IMSI)) can be *concealed* (i. e., encrypted) with the network operator's public key, yielding the so-called Subscription Concealed Identifier (SUCI) [2]. Only the operator can decrypt the identifier and thus attackers cannot derive the permanent identity anymore. Furthermore, the user's device generates a fresh SUCI for every transmission. Thereby, users should be untraceable.

This paper investigates to which extent the SUCI encryption scheme keeps its privacy promises in practice. We build upon weaknesses in the AKA procedure that enable user linkability [6–8]. We extend the existing weakness to the 5G SUCI scheme and conceptualize a SUCI-Catcher attack. As a result, the SUCI-Catcher can verify if a specific, known subscriber is present in proximity of the SUCI-Catcher, despite the encryption of the permanent identity in 5G-SA networks. Further, we scale the attack to confirm the presence of *multiple* subscribers, implement the first over-the-air SUCI-Catcher attack, and provide real-world evaluations.

In summary, our main contributions are as follows:

- We evaluate the SUPI-SUCI concealment and find that an *active* Machine-in-the-Middle (MitM) can verify the presence of an individual. We enhance the SUCI-Catcher attack to track *multiple* users, in particular, we can check for the presence of more than 500 Persons of Interest (PoI) within 60 seconds in a lab setting.
- We demonstrate the feasibility of the SUCI-Catcher in a 5G standalone network against a commercial phone. We explore the practical limits of the attack's scalability, imposed by the phone and network. Our results show that SUCI-Catchers are applicable in practice and scale well *if operators take no countermeasures like rate-limiting*. We test three networks and found they already throttle the AKA-procedure.
- We discuss the attack implication for users and possible mitigation on top of the current standard. We hope this enables operators to deploy SUCI encryption effectively and drives further security efforts within the 3GPP.

WiSec '21, June 28–July 2, 2021, Abu Dhabi, United Arab Emirates

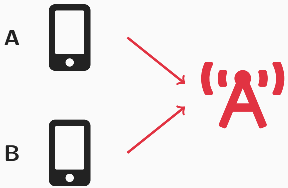
ACM ISBN 978-1-4503-8349-3/21/06.
https://doi.org/10.1145/3448300.3467826

5G SUCI-Catchers:
Still catching them all?

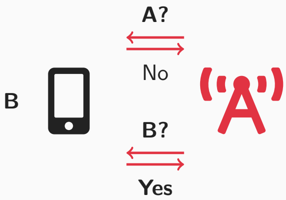
- ▶ Discover different identifiers
- ▶ Track users by testing responses
- ▶ Basics + learning by doing!

SUCI Catcher

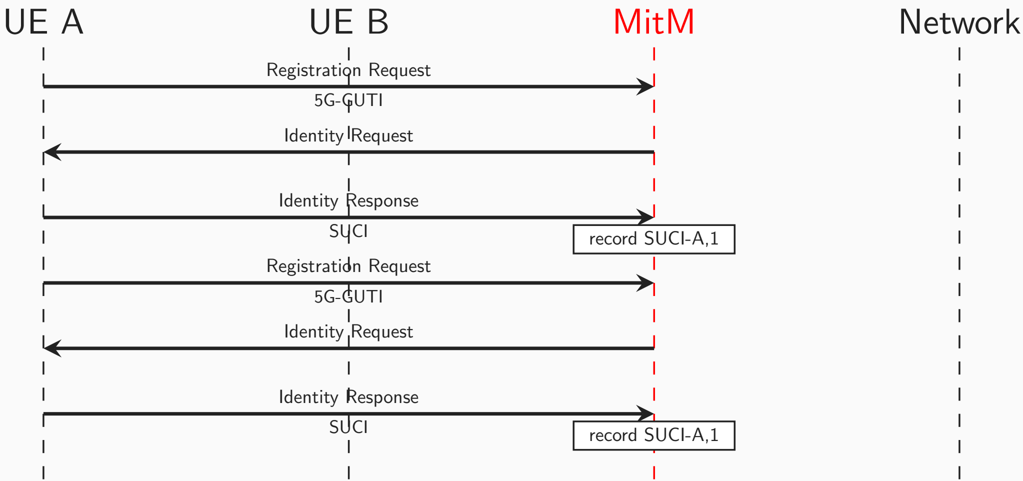
Discovery Phase



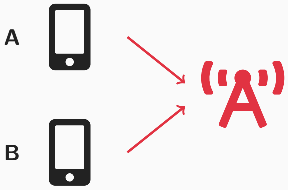
Attack Phase



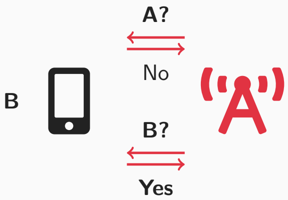
Discovery Phase — Collect SUCIs



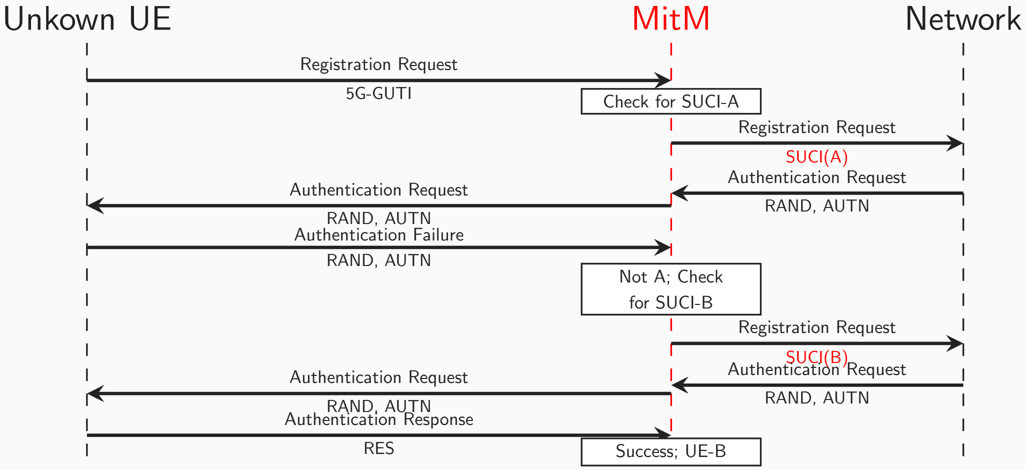
Discovery Phase



Attack Phase

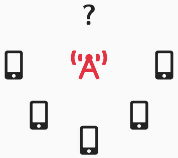


Attack Phase: Linking SUCIs



SUCI Probing Attack — Overview

- Targeted attack allows to identify a UE
- Doesn't scale with many UEs
- Rate limiting
- Depends on SIM and UE implementation



Authentication Oracle

`auth_resp.pcapng`

SUCI Catcher Attack

`suci_catcher_attack_small.pcapng`

Demo: CryptoMobile

```python
from CryptoMobile.EC import *
from CryptoMobile.ECIES import *
import binascii
# Setting up home network UDM environment
ec = X25519(binascii.unhexlify(
  'c53c22208b61860b06c62e5406a7b330c2b577aa5558981510d128247d38bd1d'))
hn_privkey = ec.get_privkey()
hn_pubkey = ec.get_pubkey()
binascii.hexlify(hn_pubkey)
b'5a8d38864820197c3394b92613b20b91633cbd897119273bf8e4a6f4eec0a650'
hn = ECIES_HN(hn_privkey, profile='A')
```

Demo: CryptoMobile

```
# Decrypting incoming SUCI A from PCAP
ue_pubkey = binascii.unhexlify(
  '7b27b315a3423f7ca10fdb77028798f86b1f58fa876cc864514a8f882d33c404')
ue_ciphertext =  binascii.unhexlify('31a0371c')
ue_mac = binascii.unhexlify('7bdd02efd7162ba2')
hn_msin = hn.unprotect(ue_pubkey, ue_ciphertext, ue_mac)
binascii.hexlify(hn_msin)

> b'00000100'
# IMSI is 208930000100 MCC and MNC in cleartext PCAP

# Decrypting incoming SUCI B from PCAP
ue_pubkey = binascii.unhexlify(
  'b34b34516dafed6973956d4cdd548d1e5d568bba76f29a9a0c17e62c28349239')
ue_ciphertext =  binascii.unhexlify('2f1fd3e7')
ue_mac = binascii.unhexlify('e158a42f076118da')
hn_msin = hn.unprotect(ue_pubkey, ue_ciphertext, ue_mac)
binascii.hexlify(hn_msin)
> b'00000101'
# IMSI is 208930000101 MCC and MNC in cleartext PCAP
```

Summary

Introduction to 5G

- The 5G wonderland
  - 20Gbps, ultra low latency
  - New use cases, new network concepts
- Improvements
  - Service-based architecture
  - User plane integrity protection
  - Interconnection security
  - Enhanced subscriber privacy
- Digging through the specification
- Decrypting SUCIs

Acronyms

5G NR	5G New Radio
5G NSA	5G Non-Standalone
5G SA	5G Standalone
5GC	5G Core
AF	Application Function
AMF	Access and Mobility Management Function
AKA	Authentication and Key Agreement
AUSF	Authentication Server Function
eNodeB	Evolved NodeB
ECIES	Elliptic Curve Integrated Encryption Scheme
EEA	EPS Encryption Algorithm
EPC	Evolved Packet Core
E-UTRAN	Evolved Universal Terrestrial Radio Access
gNodeB	gNodeB
GUTI	Global Unique Temporary Identifier
HPLMN	Home PLMN
HSS	Home Subscriber Service
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
MAC	Medium Access Control
MCC	Mobile Country Code
MME	Mobility Management Entity
MNC	Mobile Network Code
MSIN	Mobile Station Identification Number
NAI	Network Access Identifier
NAS	Non-Access Stratum
NAS-MM	NAS Mobility Management
NAS-SM	NAS Session Management
NEF	Network Exposure Function
NGAP	NG Application Protocol
NRF	Network Respository Function
NSSF	Network Slice Selection Function
P-GW	PDN Gateway
PCF	Policy Control Function
PCRF	Policy and Charging Rules Function
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PHY	Physical Layer
PRINS	PRotocol for N32 INterconnect Security
RAN	Radio Access Network
RA-RNTI	Random Access RNTI
RLC	Radio Link Control
RNTI	Radio Network Temporary Identity
ROHC	Robust Header Compression
RRC	Radio Resource Control
RTP	Real-Time Transport Protocol
SCTP	Stream Control Transmission Protocol
SMF	Session Management Function
S-GW	Serving Gateway
SEPP	Security Edge Protection Proxy
SIP	Session Initiation Protocol
SMF	Session Management Function
SRTP	Secure Real-Time Transport Protocol
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
SS7	Signalling System 7
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UDM	Unified Data Management
UPF	User Plane Function
VPLMN	Visiting PLMN