Breaking LTE on Layer 2

David Rupprecht, Katharina Kohls, Thorsten Holz, Christina Pöpper

IEEE S&P'19

Presentor : Beom Seok Oh

LTE Security Goals

- Mutual Authentication

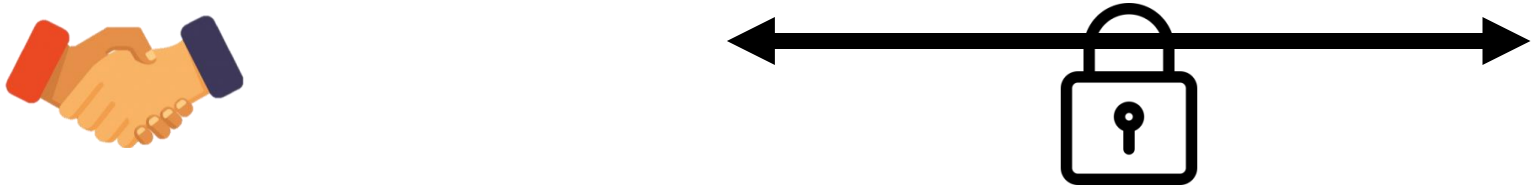
- Traffic confidentiality

- Identity & Location Confidentiality

Primitive for Security Goals

- AKA : Authentication and Key agreement procedure

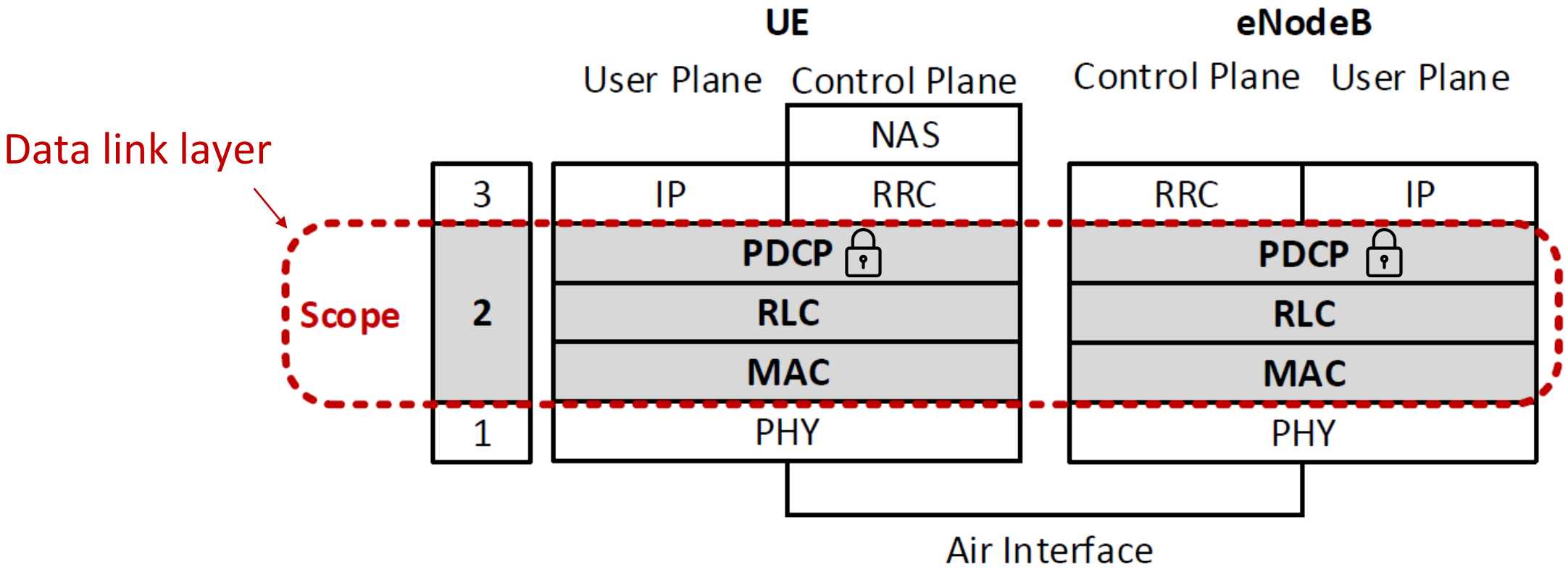
- Mutual authentication + traffic confidentiality (using shared keys).



- Still have problems?

Protection on layer two

- Where are security measures implemented?



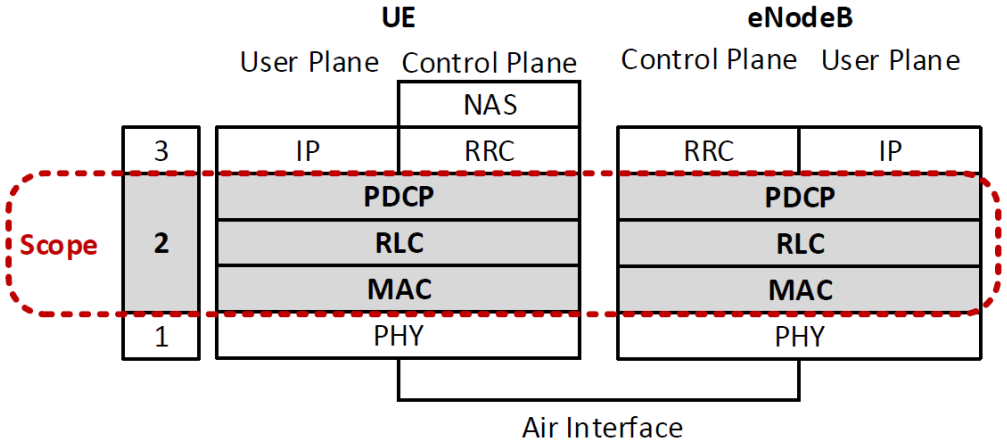
- RLC, MAC, PHY layer traffic is not confidentiality nor integrity protected.

Control vs User plane protection

- Control Plane : Controls how data packets are forwarded.
- User Plane : Carries the network user data.

- Implementations on PDCP layer

	Control Plane	User Plane
Encryption	O	O
Integrity Protection	O	X



Introduction

- Main vulnerabilities
  - Vuln1: RLC, MAC, PHY layer traffic is not confidentiality nor integrity protected.
  - Vuln2: Integrity protection is not implemented on User Plane.

- Attacks
  - Identity Mapping Attack: Vuln1
  - Website Fingerprinting Attack: Vuln1
  - aLTEr Attack: Vuln2

1. Identity Mapping Attack

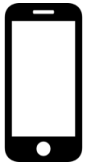
1. Identity Mapping Attack

- Identity mapping attack
  - Match permanent identity and temporary identity.
  - Match temporary identity 1 and temporary identity 2

- Why do we use temporary identities?
  - If only permanent identities are used, user activities can be tracked.
    - [GUTI Realloc paper]

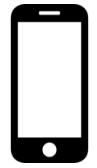
1. Identity Mapping Attack

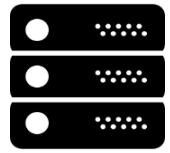
- Phone Number



82+1040325607

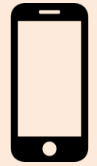
- Permanent identity IMSI

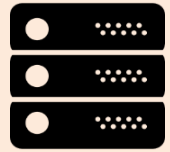





Core Network

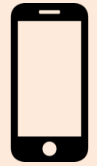
- Temporary network identity TMSI





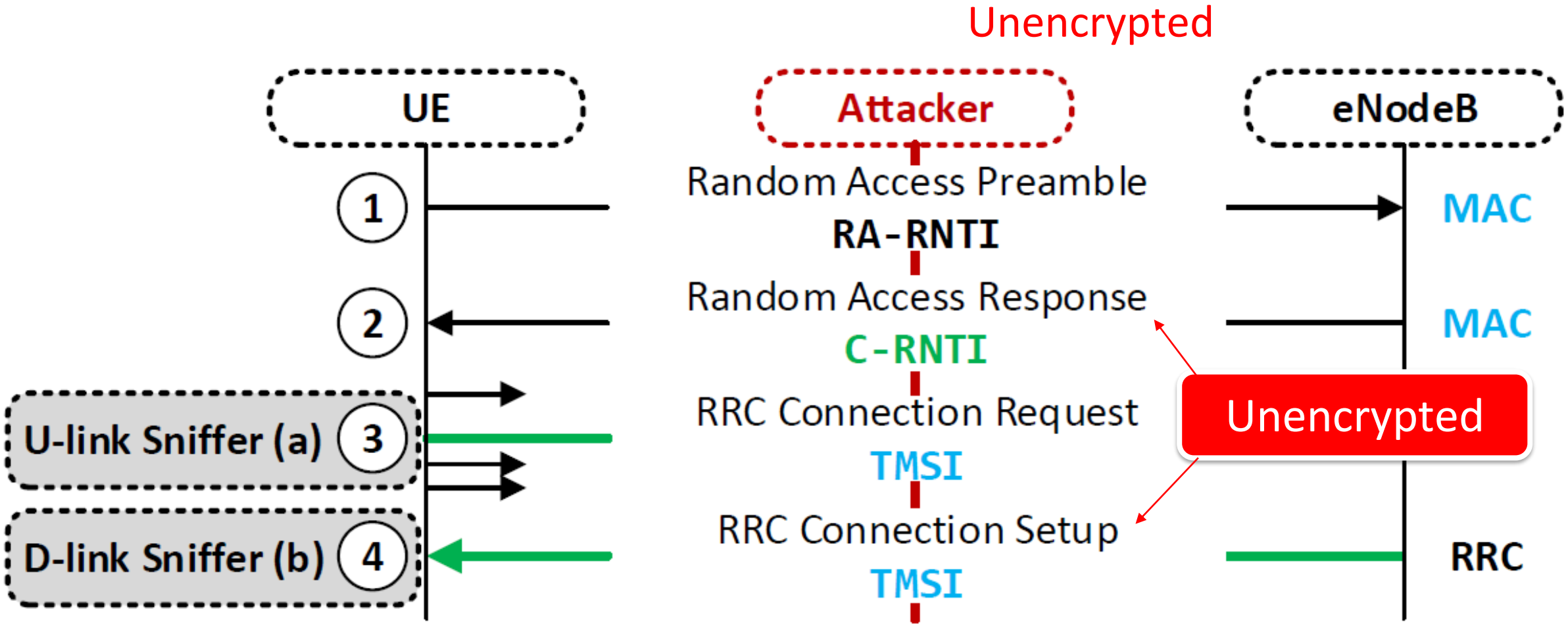
Core Network

- Temporary radio identity RNTI




Adversary maps TMSI and RNTI

1. Identity Mapping Attack

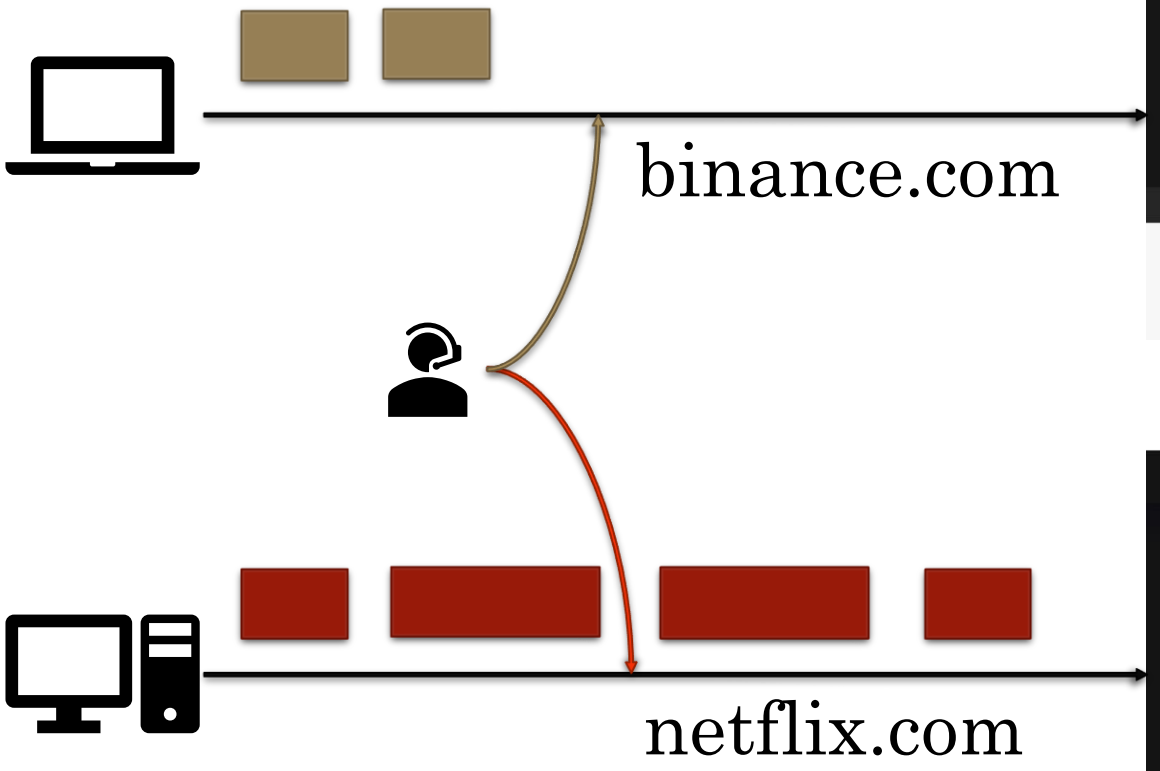


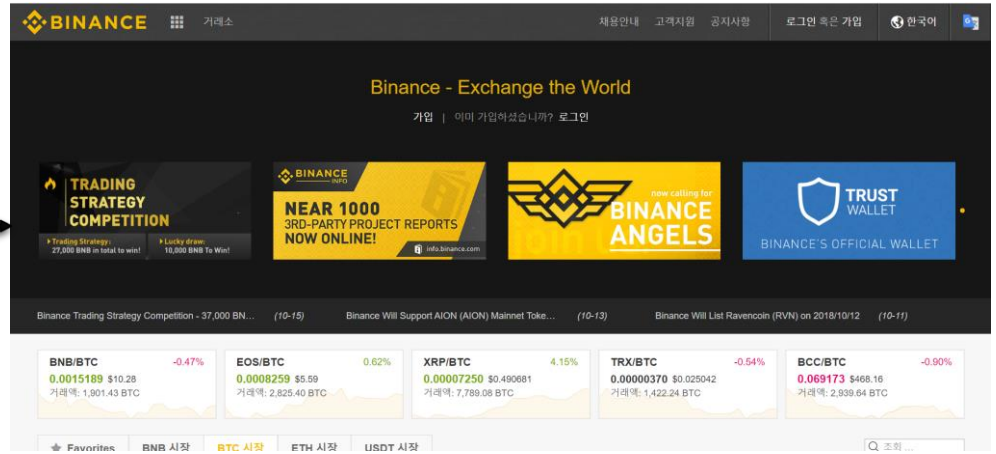
1. Identity Mapping Attack

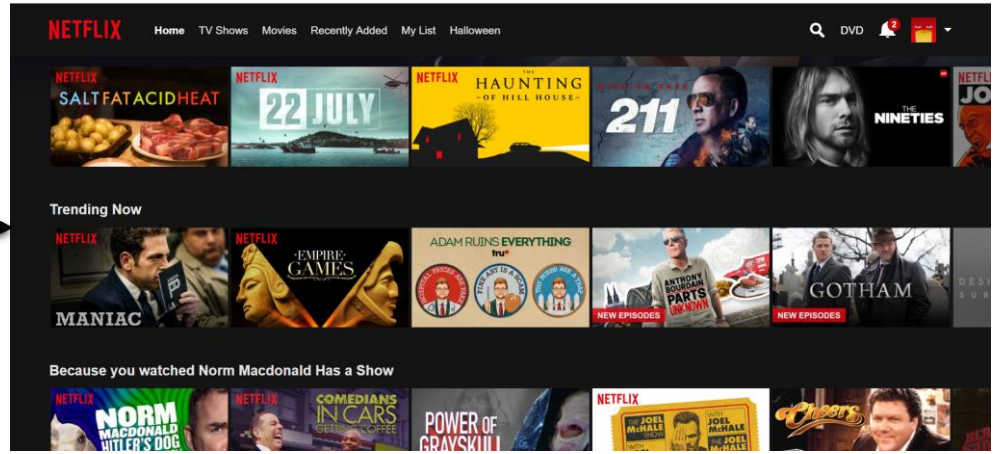
- Experiments & Results
  - Authors recorded about 96000 connection establishment procedures.
    - Using downlink sniffer
    - Eavesdropped RAR packet for C-RNTI, and RRC Connection setup message for TMSI.
  - About 95% of success.

2. Website Fingerprinting Attack

2. Website Fingerprinting Attack







2. Website Fingerprinting Attack

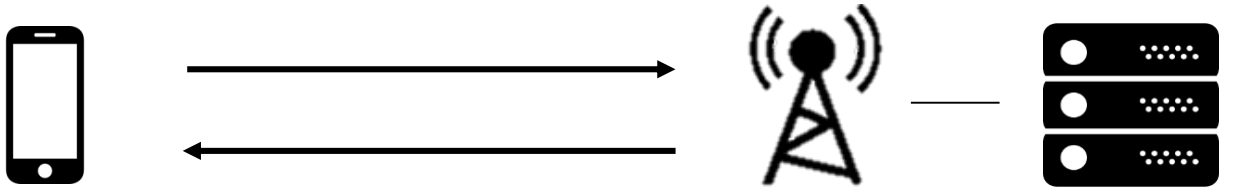
- Vulnerability : Absence of data encryption on MAC layer
  - Passive adversary can decode DCI information on MAC layer.
  - From DCI, attacker learns user data traffic and gain metadata features.
    - Can distinguish requests to different websites.
    - E.g. Length of PDCP packet, timing patterns of transmissions

- Attack procedure
  1) Create a training set of user traffic, accessing to multiple websites.
  2) Apply Fast Dynamic Time Warping (DTW) to the set.
  3) Classification attack

Computes similarity of two time series

2. Website Fingerprinting Attack

- Experiments



  - Collected user plane traffic at eNB.
  - Used 3 Android phones.
  - Accessed to Alexa top 50 websites, overall 100 times with each phone.

- Result : About 90% success rate for both uplink and downlink.

3. aLTEr Attack

3. aLTEr Attack

- aLTEr attack
  - Manipulates known part of encrypted LTE user traffic.

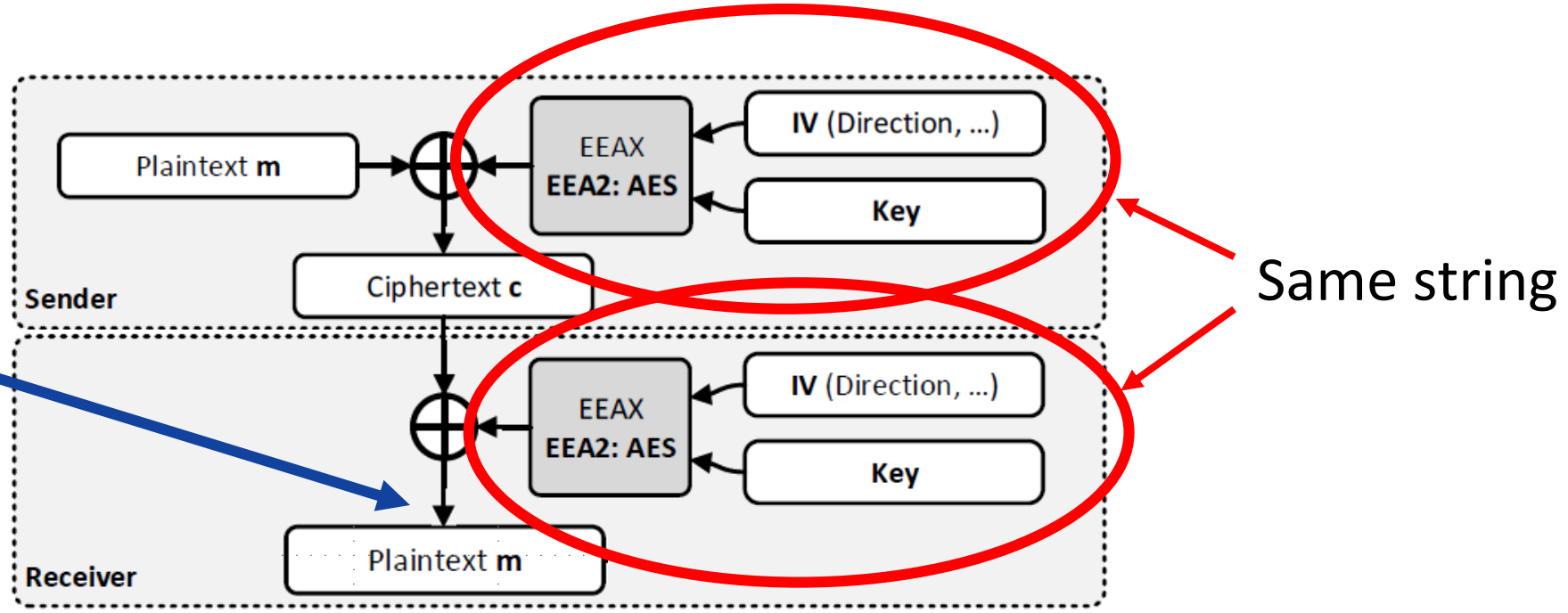
- Vulnerability
  - Lack of integrity protection on user plane.
  - Encryption on LTE user data is performed by block ciphering in counter mode.

	Control Plane	User Plane
Encryption	O	O
Integrity Protection	O	X

3. aLTEr Attack

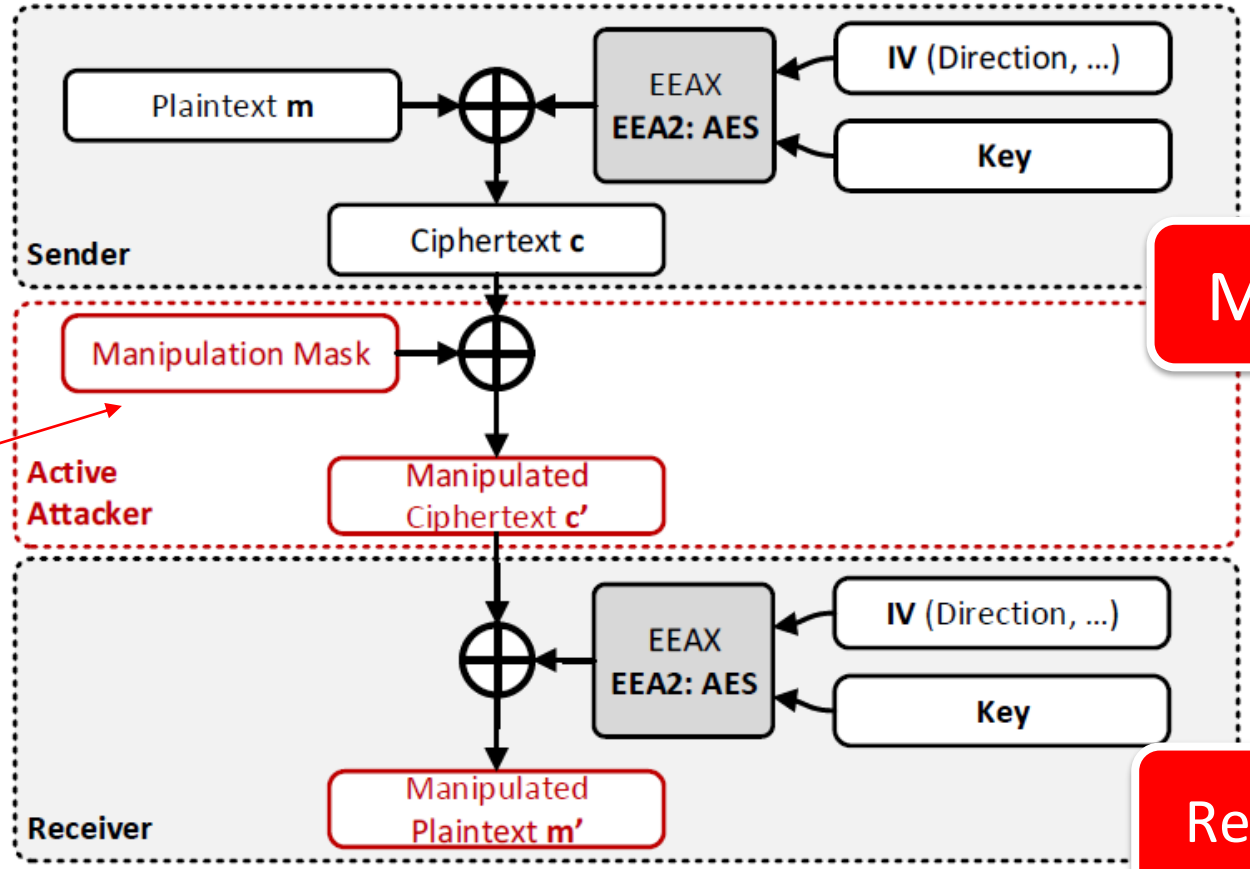
- Data encryption – AES CTR

$X \oplus X \oplus Y = Y$



3. aLTEr Attack

- Packet modification
  - Known plaintext m, manipulated text m'.



Mask = m ⊕ m'

Inserted block by an attacker

Result = MASK ⊕ m

3. aLTEr Attack

- Found that adversary can deliver manipulated user plane traffic to receiver.
  - But original text should be known.

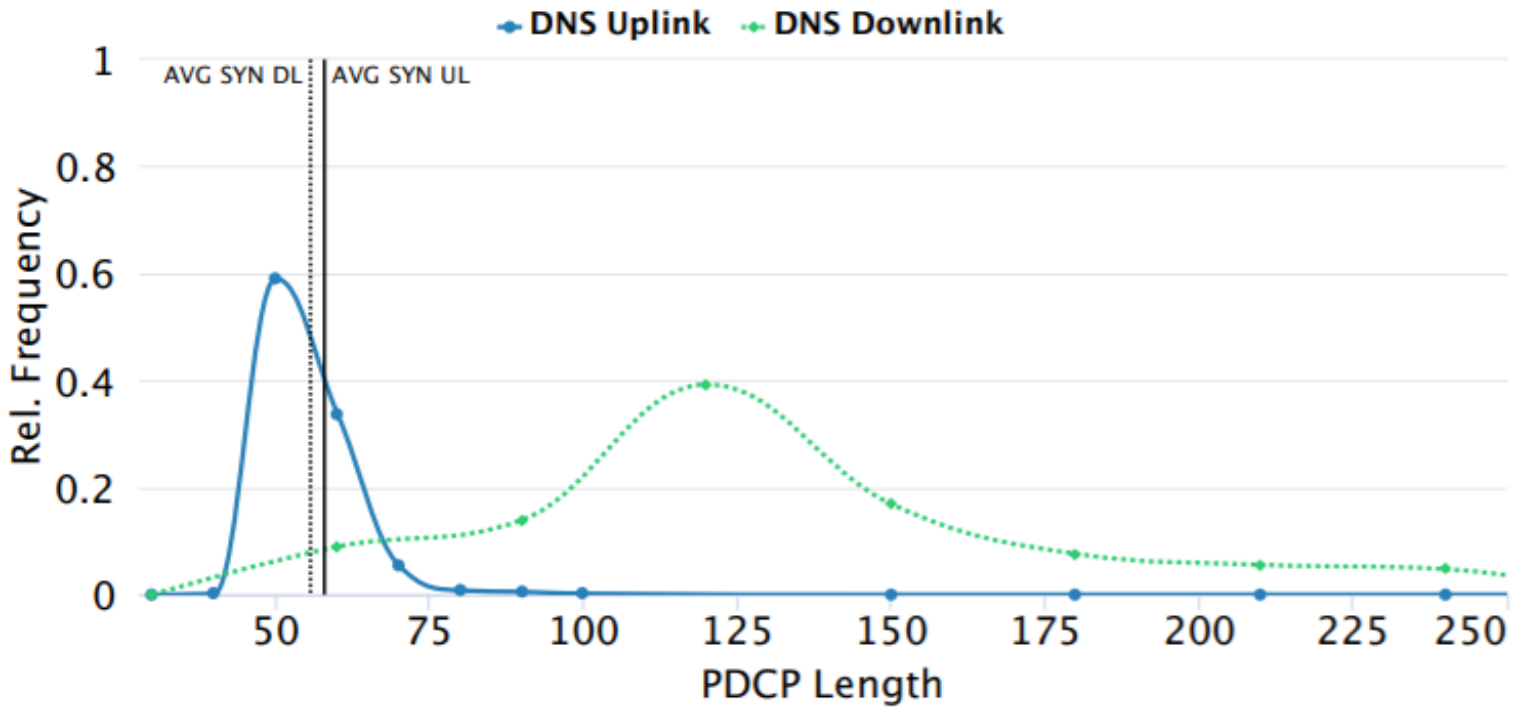
- Two challenges to design attack.
  - Chall1 : Selection of target traffic
    - How to distinguish target from encrypted user traffic?
  - Chall2 : Selection of target text to manipulate
    - Original text should be known.
    - Attack should be performed by the modification.

1. Select DNS request/response as target.

2. Modify destination (and source) IP address

3. aLTEr Attack

- Overcome challenge 1 : Select DNS request/response as target.
  - DNS requests/responses are distinguishable from user traffic.
  - Using PDCP length as a feature, about 96% of accuracy.



3. aLTEr Attack

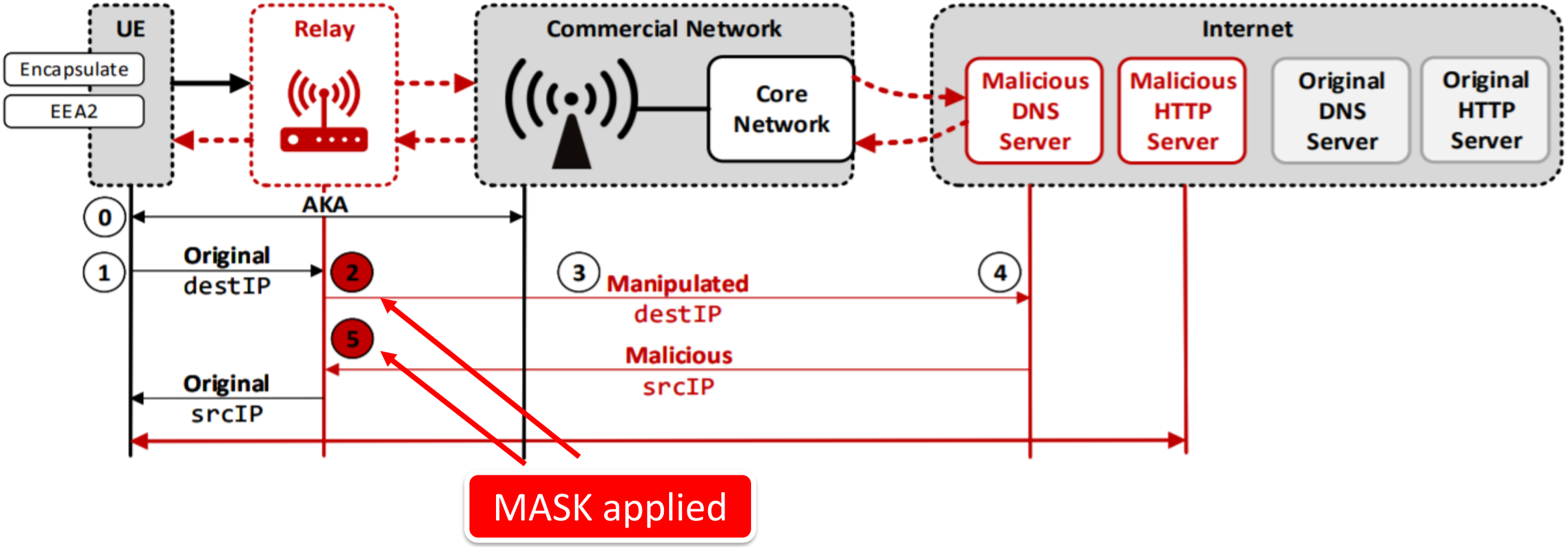
- Overcome challenge 2 : Modify IP address
  - By changing IP address, DNS redirection attack can be performed.

	DNS request	DNS response
Destination IP address	Known	
Source IP address		Known

- Modify IP address to redirect DNS request.
  - Also hide source of DNS response.

3. aLTEr Attack

- Overview of the attack procedure



3. aLTEr Attack

3. aLTEr Attack

- Defense
  - Update standard so that integrity protection is provided to user plane data.
    - Why integrity protection is not used on user plane?
    - Increase of packet size, due to MAC.

IMP4GT Attack – Follow up study

- D. Rupprecht, K. Kohls, T. Holz, and C. Popper, “IMP4GT: Impersonation attacks in 4G networks,” in Proc. ISOC NDSS, Feb. 2020
  - Impersonation attack
    - Send packet to HTTP server with victim’s identity.
  - First perform aLTEr attack and use encryption/decryption oracle authors made.
    - Attack is possible due to same vulnerabilities.

User Plane Integrity Protection

- Taking a look on standard : 3GPP standard of LTE & 5G
  - **LTE : 33.401**

> 5.1.4 User data and signalling data integrity
>
> 5.1.4.1 Integrity requirements
>
> User plane packets between the eNB and the UE shall not be integrity protected on the Uu interface. User plane packets between the RN and the UE shall not be integrity protected. All user plane packets carrying S1 and X2 messages

  - **5G : 33.501**

> The gNB shall support integrity protection and replay protection of user data between the UE and the gNB.
>
> Integrity protection of the user data between the UE and the gNB is optional to use,

Conclusion – Wrap up

- Identity Mapping Attack
  - Map RNTI and TMSI.
  - Identify and localize users in network.

- Website Fingerprinting Attack
  - Learn accessed website from metadata of encrypted traffic.
  - Distinguish accessed websites.

- ALTER Attack
  - Manipulates known part of encrypted LTE user traffic.
  - Redirection of DNS request from user.

Questions – Q1

- Best Question : (Junho Ahn) I heard that specification is changed because of this paper. However, it is not mandatory to use but to support integrity protection on UE. Is aLTEr attack blocked because of changed specification or still possible?
  - For UE, required to support full-rate integrity protection of user data.
  - However, it's hard for eNB to support full rate integrity protection.
  - 5G full-rate speed : 20Gbps / gNB : 2Tbps for 100 UE
  - In summary, UE is mandatory to support full-rate integrity protection, but not mandatory for gNB. Thus, aLTEr attack can be performed still.

Questions – Q2

- Best Question : (Gyu-hwan Park) I want to know the detailed method of their experiment. Are the devices they used as UE or eNodeB using the system used by actual telephony companies?
  - For website fingerprinting & aLTEr attack : Commercial UE
  - For identity mapping attack : srsUE
  - srsRAN is a 4G/5G software radio suite developed by SRS.
    - srsUE - 4G/5G-NSA UE application (5G-SA coming soon)
    - srsENB - 4G/5G-NSA eNodeB application (5G-SA coming soon)
    - srsEPC - 4G core network implementation with MME, HSS and S/P-GW

Questions – Q3

- (Kyung-tae Kim) Does DNSSEC protect aLTEr attack?
  - aLTEr attack manipulates known part of encrypted LTE user traffic.
  - Rather than DNS traffic & IP address, there can be other targets.
  - Specifically, DNSSEC can protect aLTEr attack introduced in this paper.
  - However, if target is not DNS traffic? It won't.

  - In summary : Yes, it can. But it's not fundamental solution.
    - Vulnerabilities are not covered by DNSSEC.