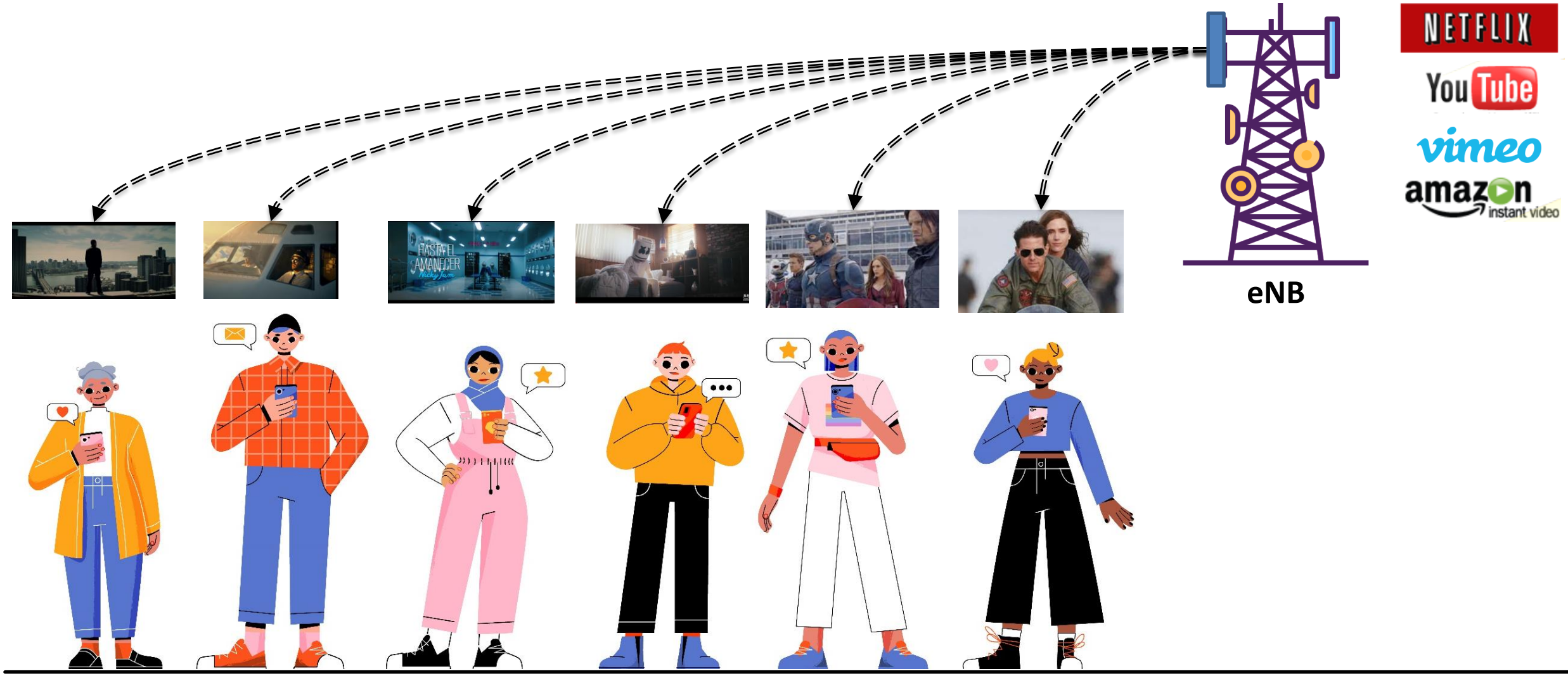
USENIX Security 2022

Watching the Watchers: Practical Video Identification Attack in LTE Networks

Sangwook Bae, Mincheol Son, Dongkwan Kim, CheolJun Park, Jiho Lee, Sooel Son, and Yongdae Kim

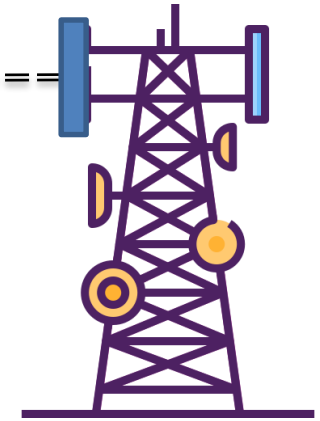
KAIST

We Now Use Smartphone To Watch Videos



What Someone Watches Reveals Who They Are

.....



eNB

NETFLIX

YouTube

vimeo

amazon instant video

Video Privacy Protection Act (VPPA)

"wrongful disclosure of video tape rental or sale records"

Someone's watching history is privacy-critical information

Watching the Watchers?

Q1. Can the adversary identify the video that victim is watching without any access?

Q2. Can we physically expose victims watching a particular video?

Is Video Traffic Fingerprintable?

Usenix Security '17

Beauty and the Burst:
Remote Identification of Encrypted Video Streams *

INFOCOMM '18

Walls Have Ears: Traffic-based Side-channel Attack in Video Streaming

Jiaxi Gu*, Jiliang Wang†, Zhiwen Yu*, Kele Shen†
*School of Computer Science, Northwestern Polytechnical University, P.R. China
†School of Software, Tsinghua University, P.R. China
gujiaxi@mail.nwpu.edu.cn, jiliangwang@tsinghua.edu.cn, zhiwenyu@nwpu.edu.cn, sk116@mail.tsinghua.edu.cn

TIFS '17

I Know What You Saw Last Minute—Encrypted HTTP Adaptive Video Streaming Title Classification

Ran Dubin, Amit Dvir, Ofir Pele, and Ofer Hadar, *Senior Member, IEEE*

Codaspy '17

Identifying HTTPS-Protected Netflix Videos in Real-Time

Andrew Reed, Michael Kranch
Dept. of Electrical Engineering and Computer Science
United States Military Academy at West Point
West Point, New York, USA
{andrew.reed, michael.kranch}@usma.edu

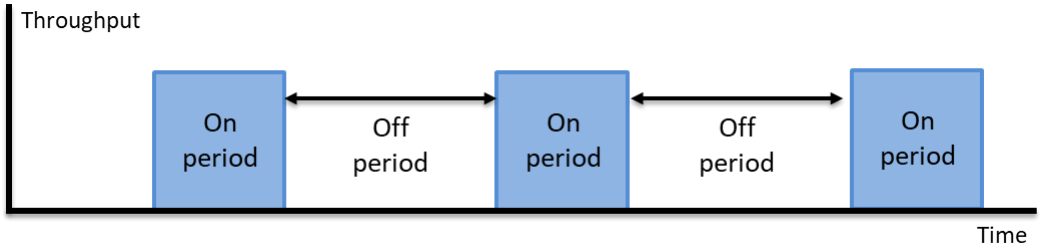
.....

Video identification attack
through traffic analysis
over the encrypted traffic in ***wired network***

How? → HTTP adaptive streaming (HAS)'s working logic generates fingerprint

- Video is segmented into smaller chunks
- Chunk's sizes vary according to the content due to VBR

→ ***Produce distinctive On-Off traffic pattern***



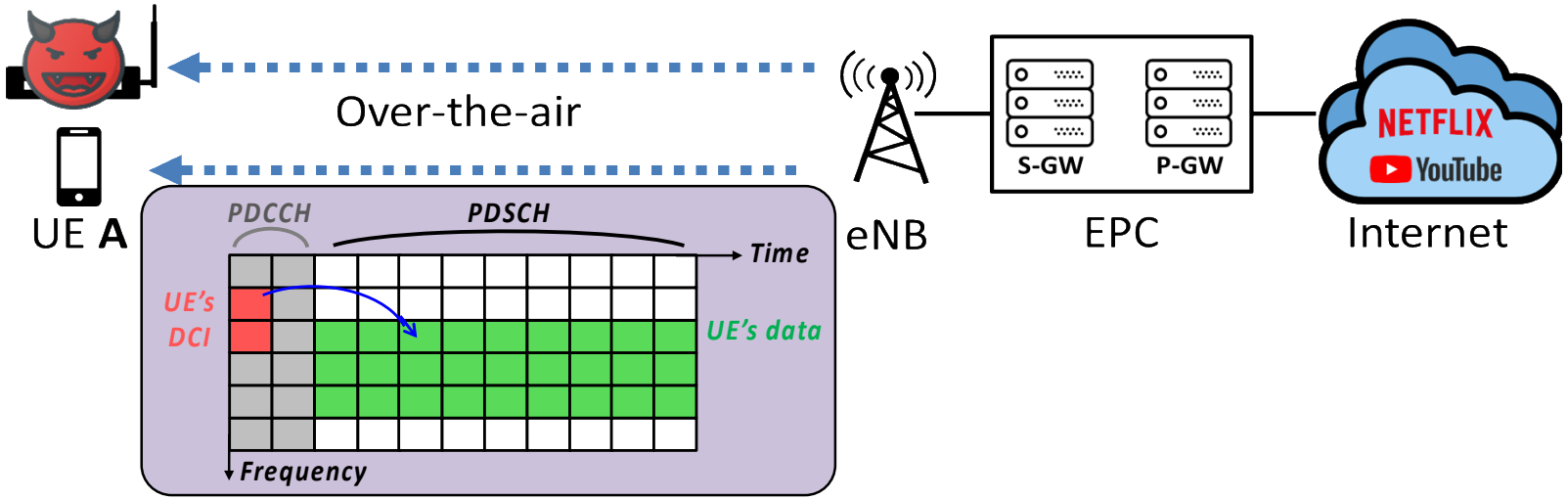
They are required to
1) **Direct access to a victim's network infrastructure**
2) **Ability to run malicious apps or websites in a victim's device**

SysSec System Security Lab

Can Adversary In LTE Monitor The Victim's Traffic?

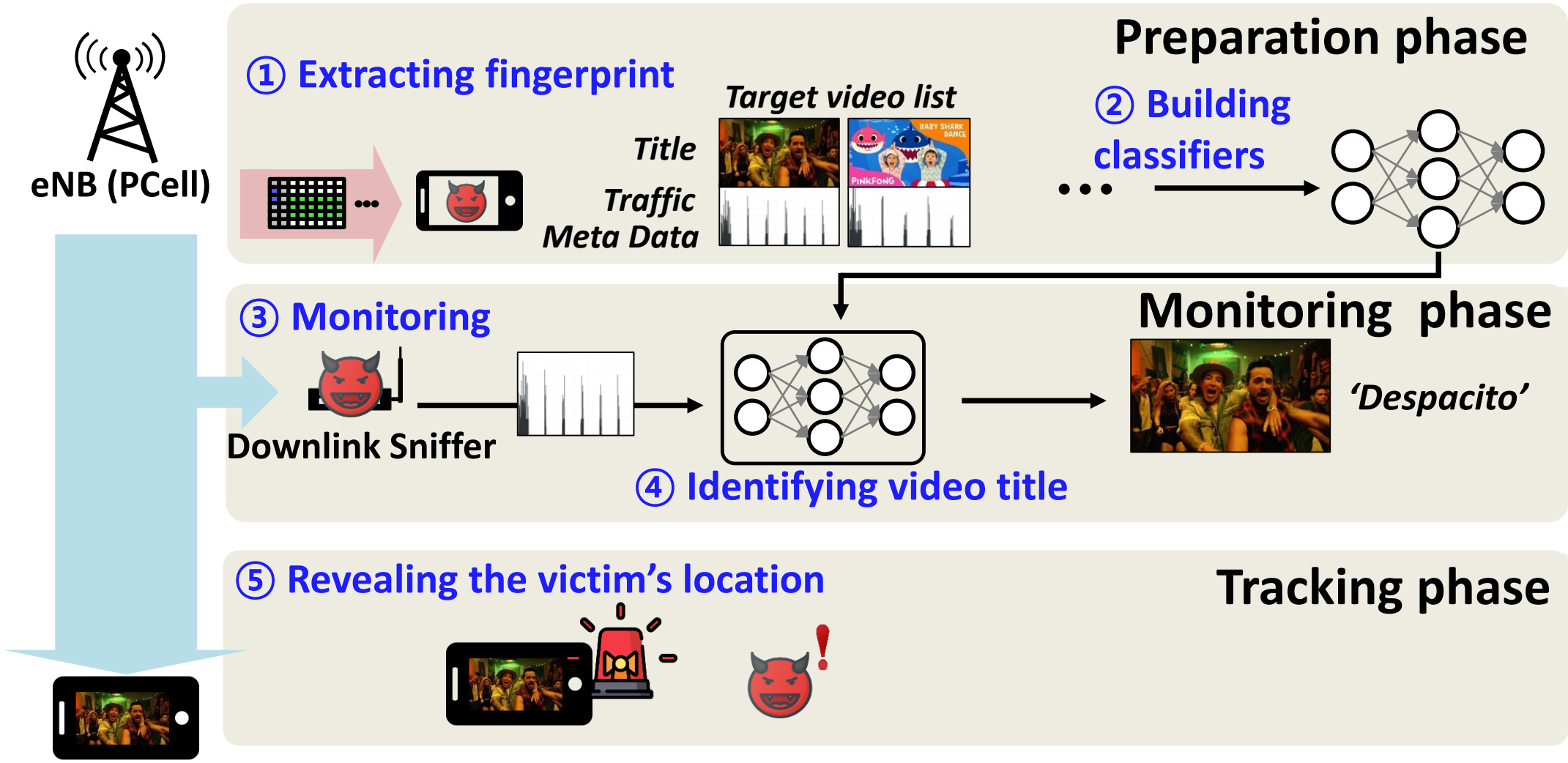
- In LTE, unprivileged adversary can monitor the victim's downlink traffic.
- eNB (base station) controls DL data transmission by broadcasting DCI
- Downlink Control Indicator (DCI)
  - Descriptions about DL data transmitted to the UE
    - Data volume, modulation scheme, allocated resource blocks (RB)
  - Distinguished by RNTI (radio network temporal Identifier)

This information is broadcast in plain text

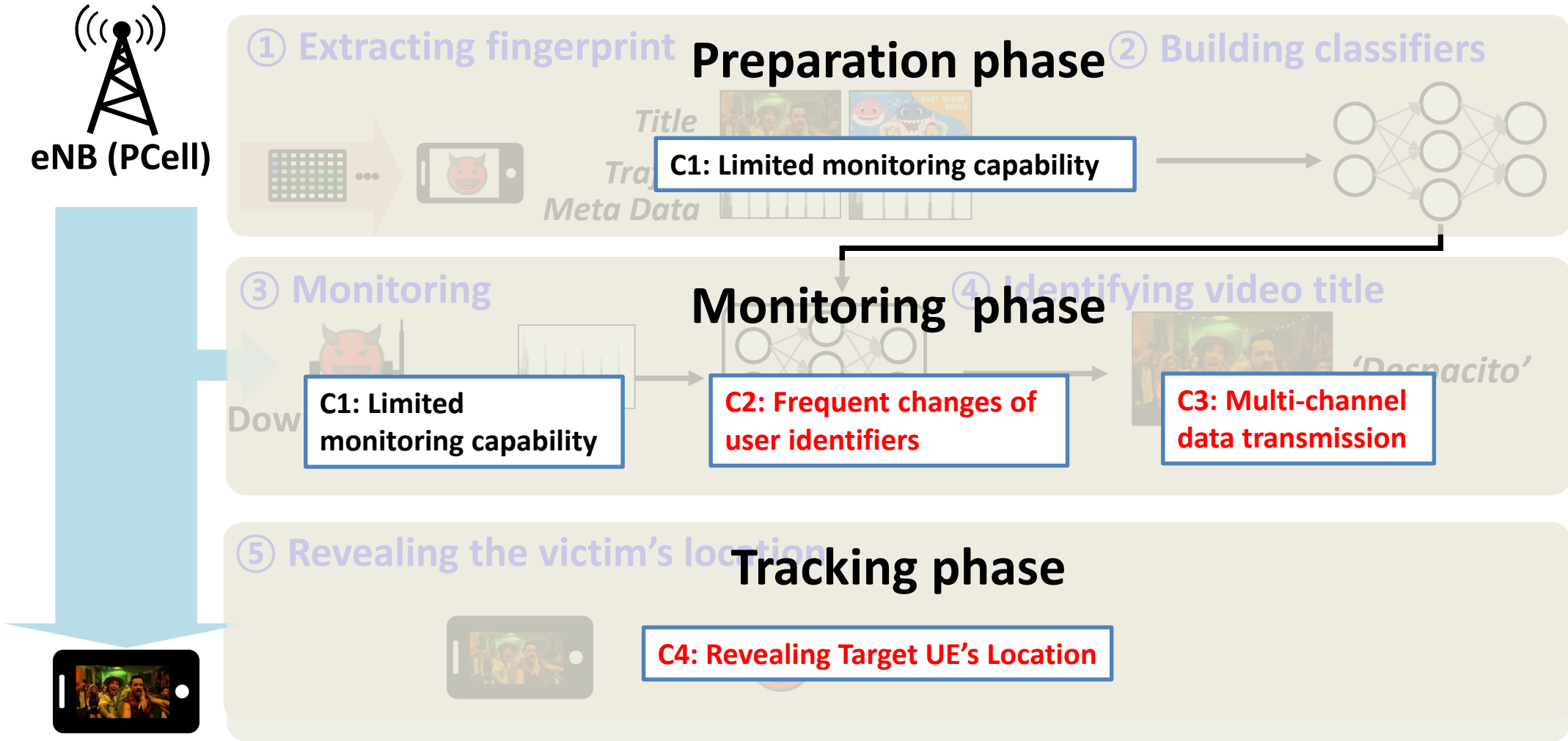


SysSec System Security Lab

Overall Procedure



Challenges of Video Identification Attack in LTE



C2: Frequent Changes of user identifiers

HAS

During OFF period, there is no data transmission

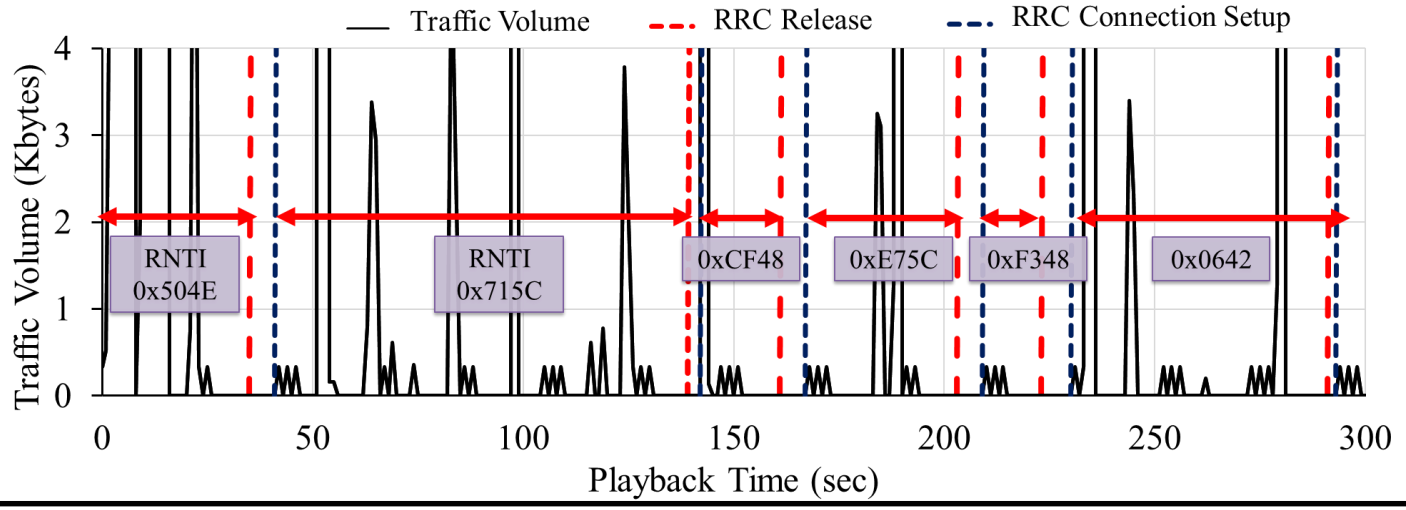
+

LTE

UE releases its connection to an eNB when there is no traffic for a certain period (~10s)

UE's RNTI is changing during the video streaming at (every) OFF period

Time series of received traffic volume and the changing RNTIs when a client plays a Netflix video*

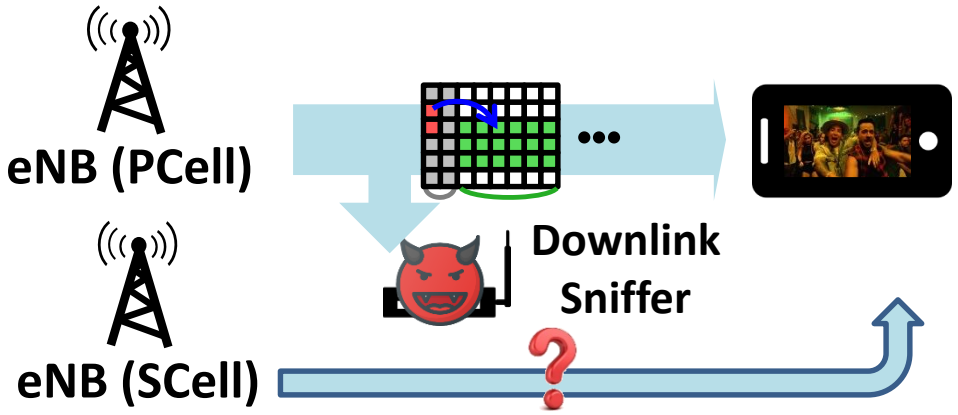


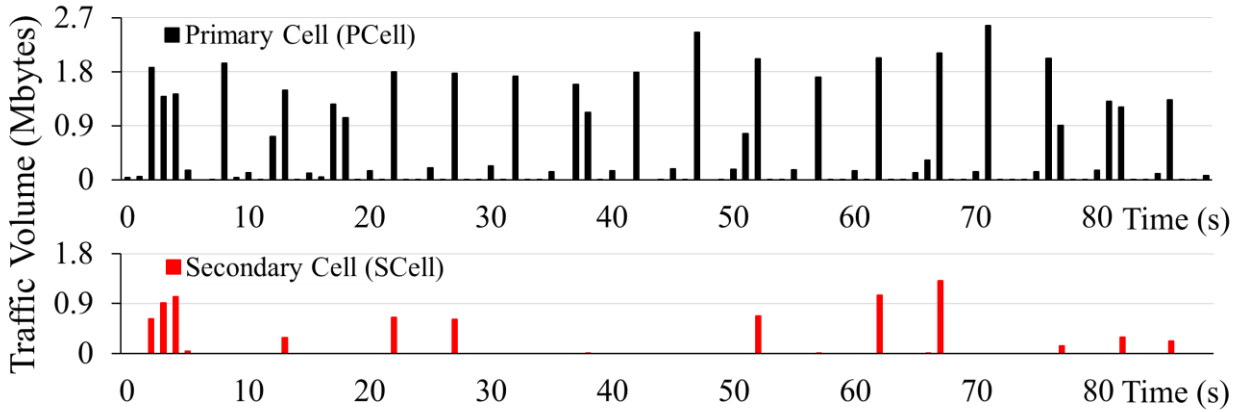
*Sherlock (Season 1, EP. 1)

C3: Multi-channel Data Transmission

- Carrier aggregation (CA)
  - Deliver a large volume of data over multiple channels (secondary cells: SCell)
- large amount of data is likely to be transmitted using CA
  - A typical streamed video consists of large video chunks

Single downlink sniffer loses the traffic information





SysSec System Security Lab

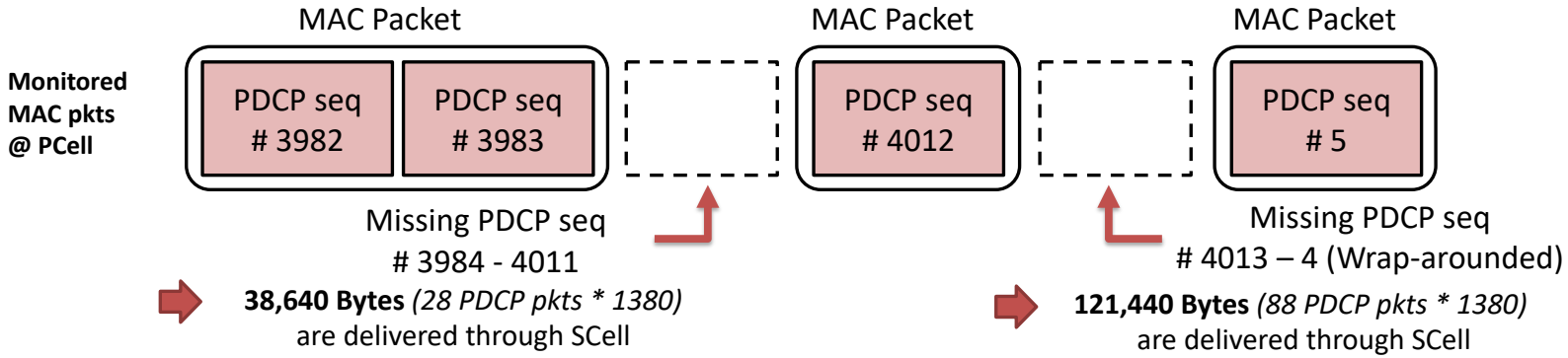
Utilize Broadcast/Exposed Information

C2: Frequent changes of user identifiers
- RNTI is changing during the video streaming

C3: Multi-channel data transmission
- Data is delivered through unmonitored cell

Utilize broadcast information
- Exposed Temporary/ (semi) permanent identifier
- Unencrypted packet header

- Temporary and (semi) permanent identifiers are exposed at the same message
  - GUTI is temporary identifier, but it is not changed frequently
  - → **Track the identifier (RNTI) by monitoring RNTI allocation procedure**
- Estimate the traffic volume with only one SDR device at PCell
  - Unencrypted packet header information in PDCP & MAC

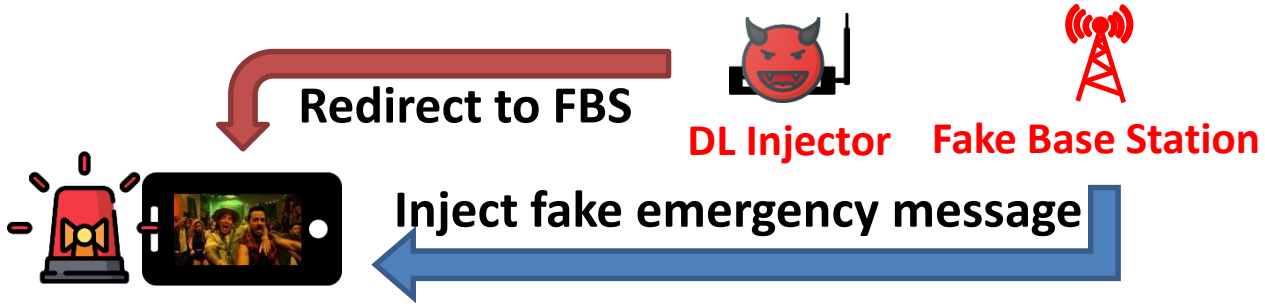


Utilize Unprotected Protocol Layer (PHY)

C4: Revealing target UE's location

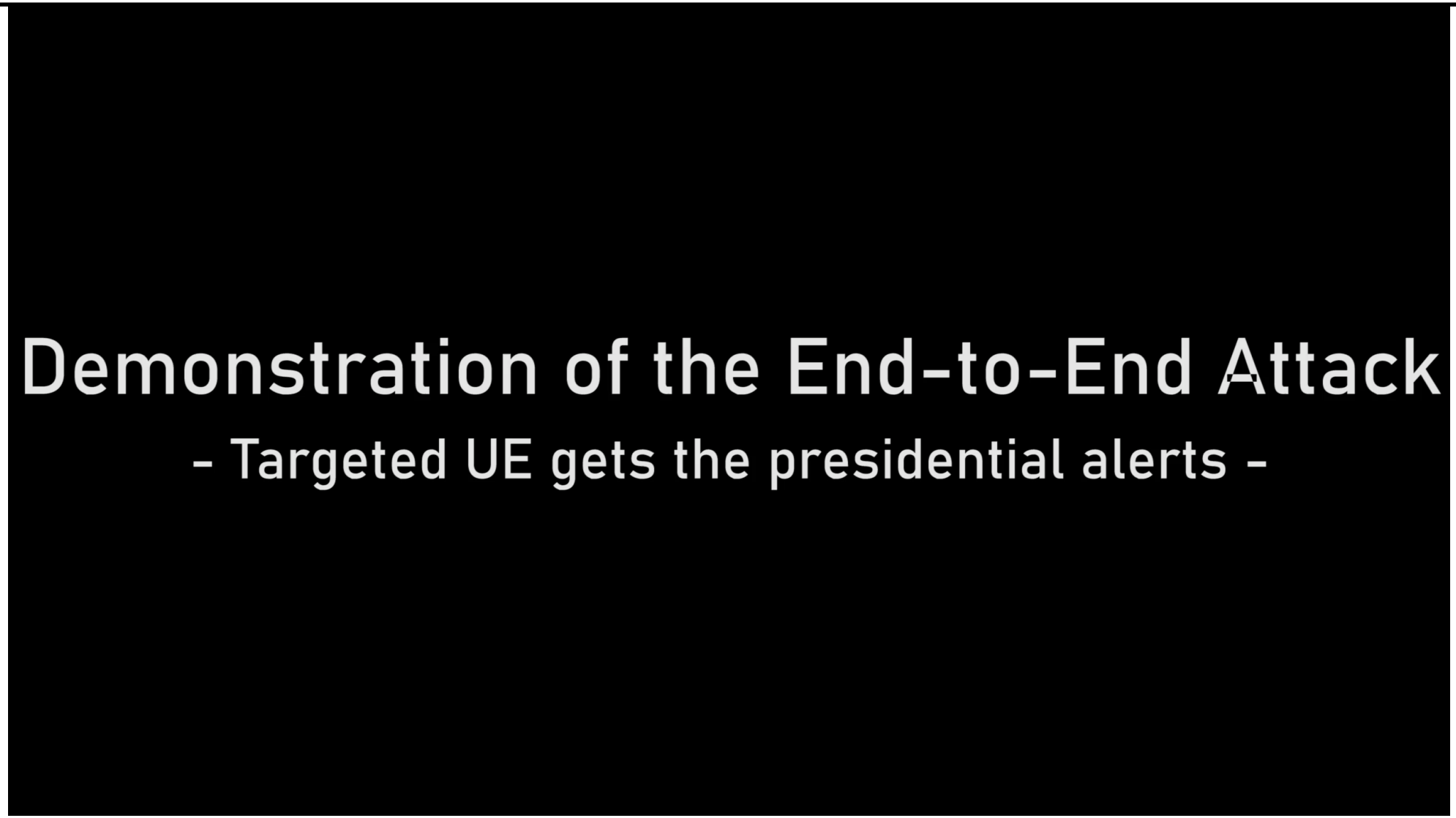
Utilize unprotected protocol layer (PHY)
- Inject targeted emergency SMS

- Key purpose: only the target UE receives the presidential alert
- Force target UE to redirect to FBS by injecting malicious control plane messages
  - Extend **signal overshadowing attack** (SigOver) [USENIX 19]
- FBS sends fake emergency message to the target UE
  - FBS operates in unused frequency
- UE makes a loud alarm → revealing its physical presence



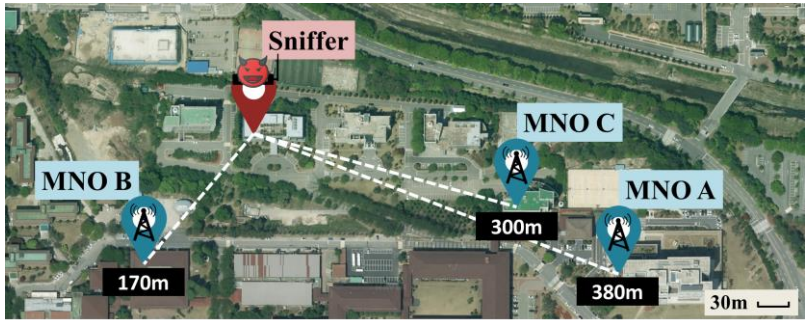
Hojoon Yang, **Sangwook Bae**, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim. "Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE" in USENIX 19

Demo


Demonstration of the End-to-End Attack
- Targeted UE gets the presidential alerts -

Dataset & Implementation

- Total of 46,810 data traces
  - **2,035 hours** of streaming time, 1.79 TB of video traffic
  - **3 operational MNOs** in Korea
  - Types and # of video titles (class size)
    - Video traffic: YouTube (300), Amazon (68), and Netflix(50)
    - Non video traffic: web surfing (Alexa Top 50), teleconference (Google Meet)
  - **Three different resolution**: 480, 720, 1080p



- Implementation
  - Downlink sniffer: AirScope and Optis-S DM analyzer
  - Video title identifier: CNN classifier
    - Keras with a TensorFlow backend
  - Video service type identifier: decision tree
    - Python Scikt-learn

Conclusion

- Watching the watchers: Video identification attack
  - LTE design **exposes a lot of information**
  - Unprivileged attacker can monitor the victim's traffic **without any access**
  - Especially, there are unique challenges in the video streaming through the LTE
  - Cellular network enables more critical privacy threatening attack
    - Unprivileged attacker can revealing the victim's presence

- We open our dataset (over **2,035 hours** of streaming) & codes

  (Dataset & codes for data collection) https://github.com/SysSec-KAIST/WatchingTheWatchers

  (Unicast message injection) https://github.com/SysSec-KAIST/sigover_injector

- Questions?
  - Sangwook Bae: baesangwook89@gmail.com (@baesangwook89)