CCIT 네트워크 발표

- 패킷 조작을 통한 통신사 데이터 과금 방지

CCIT 정보보안SW전공

장한빈

CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

Contents

통신사 데이터 과금 방식

1. 통신사 데이터 과금 방식

- UDP 통신 외 기타 프로토콜
  - 송 수신된 패킷의 데이터 길이를 측정하여 길이만큼 데이터 과금

취약점

- TCP 통신
  - 송 수신된 패킷의 데이터 길이를 알 수 있는 특별한 값(Seq Number)를 통해 데이터 과금
  - 재 송신 된 패킷(Retransmisson)에 대해 추가 과금을 부여하지 않음

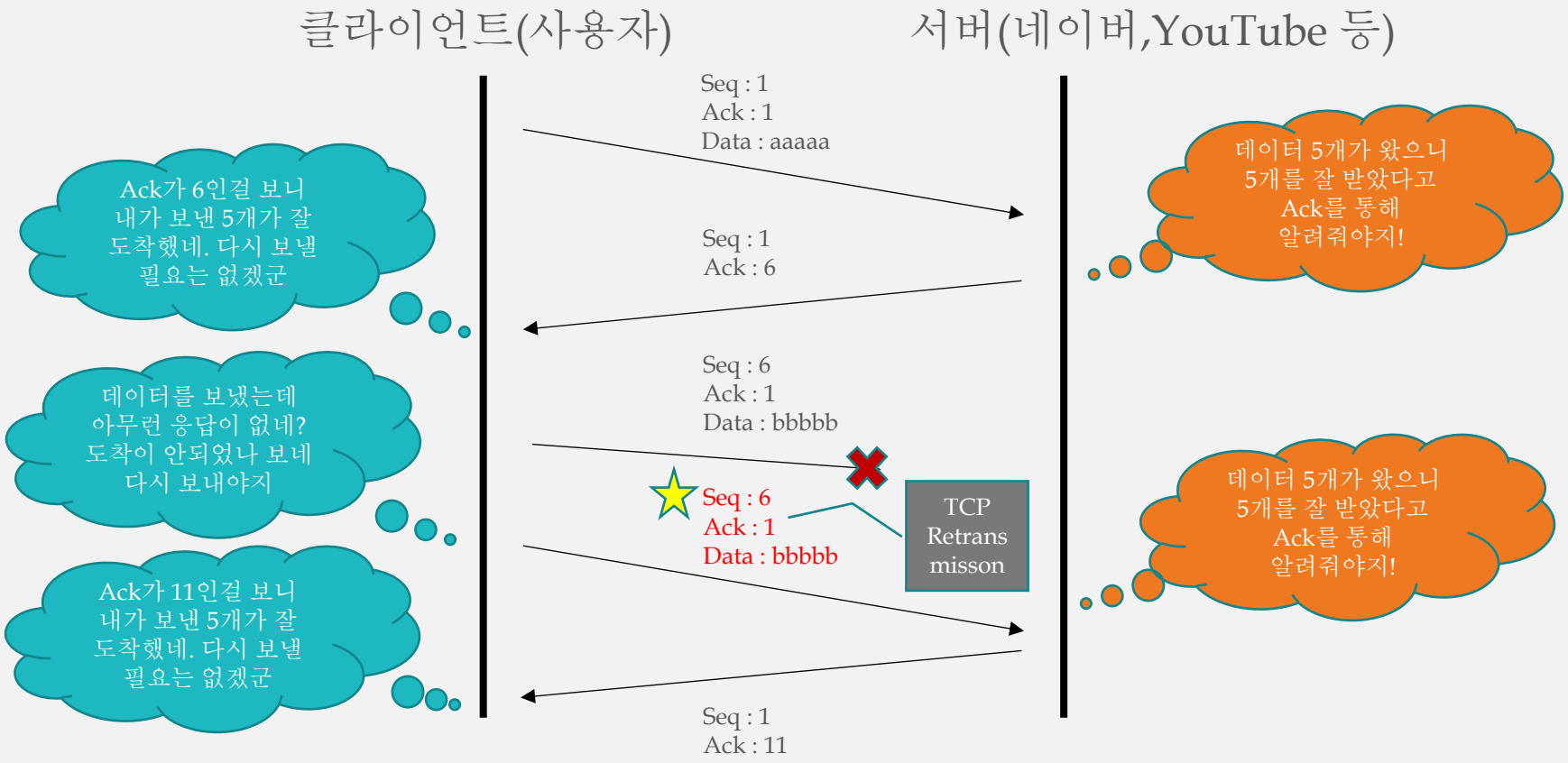
1. 통신사 데이터 과금 방식

1. 통신사 데이터 과금 방식

- Packet 이란?
  - 컴퓨터 네트워크에서 데이터를 전달하는 블록 단위를 말함.

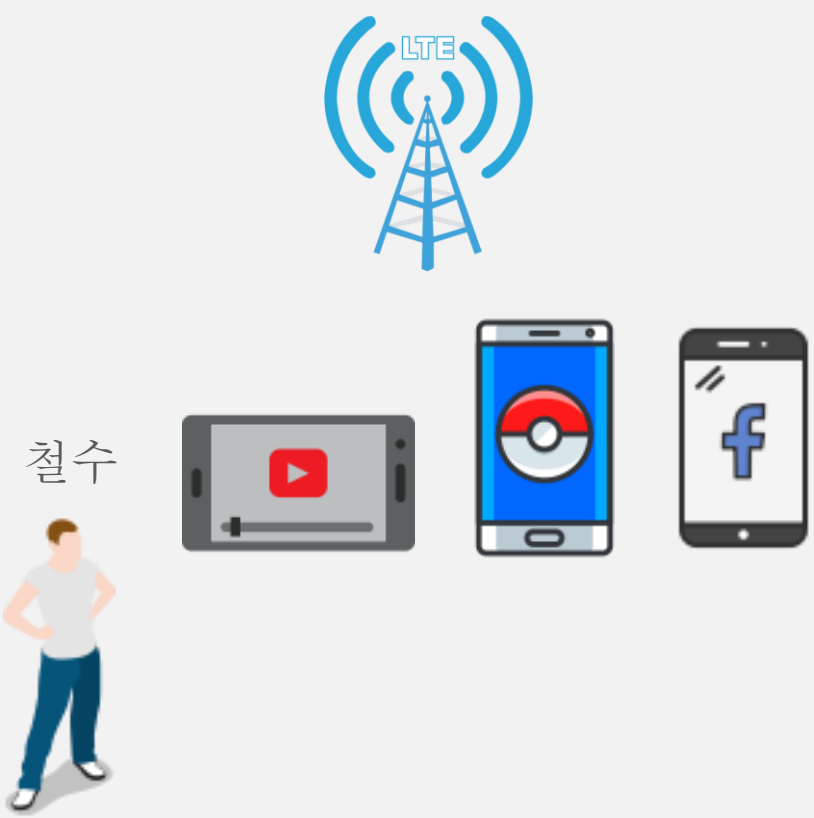
- TCP 란?
  - Transmission Control Protocol의 약자로 전송 제어 프로토콜을 뜻한다.
  - 흐름제어, 오류제어가 가능하여 신뢰성 있는 연결을 하게 해준다.
    - 즉, 패킷의 전송이 누락되거나 잘 못 되었을 경우 전송한 패킷을 온전히 받을 수 있도록 재 전송한다.

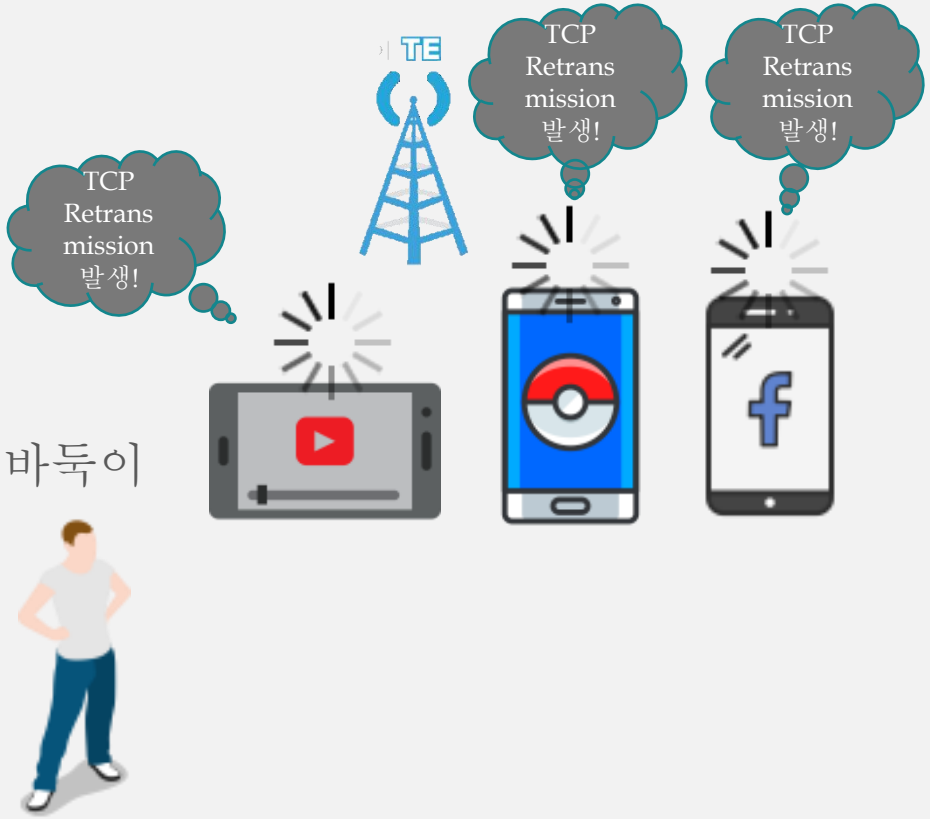
1. 통신사 데이터 과금 방식



1. 통신사 데이터 과금 방식

만약 현재 과금 정책을 사용하지 않는다면 ?





1. 통신사 데이터 과금 방식

만약 현재 과금 정책을 사용하지 않는다면 ?

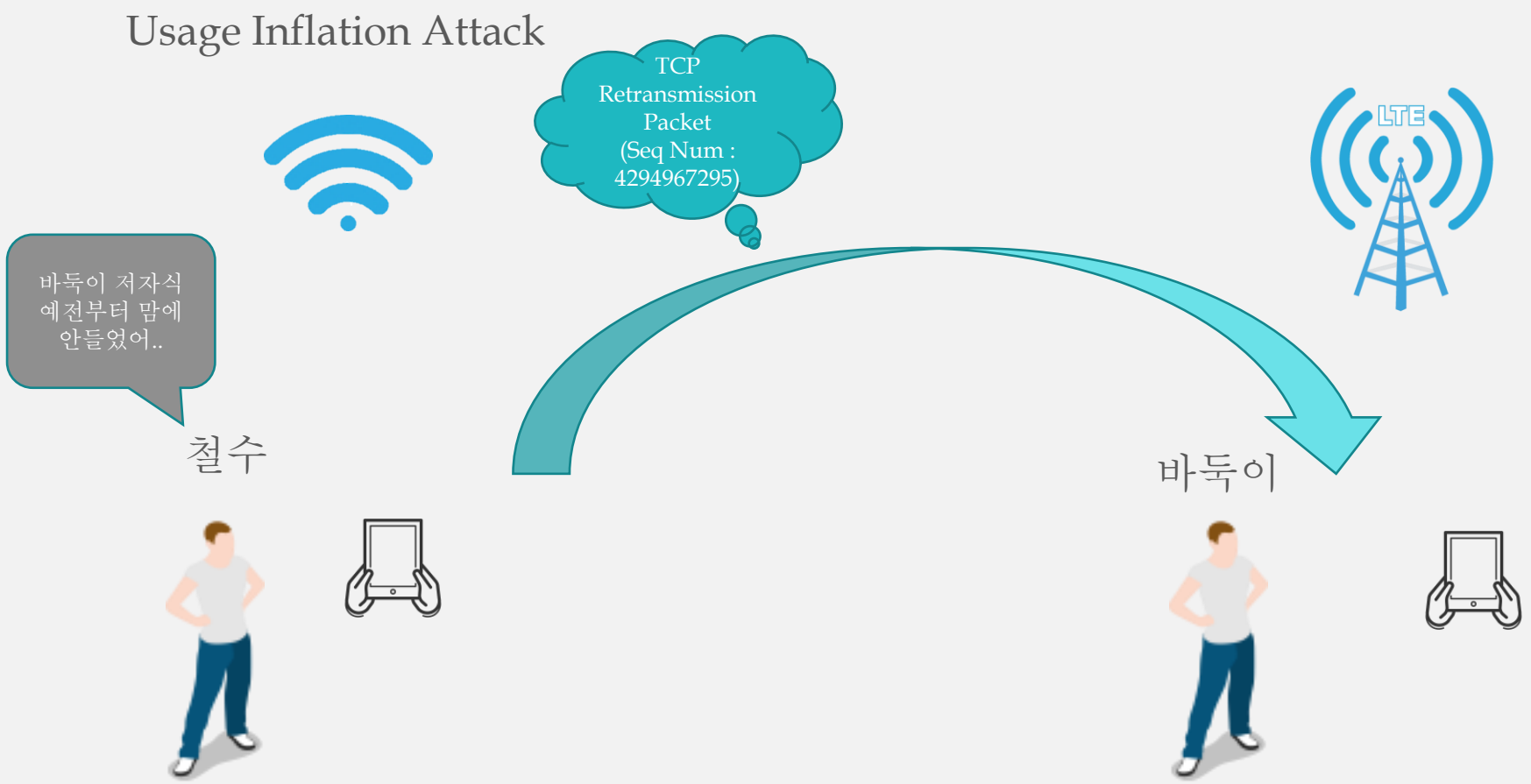
통신 요금 납부서

철수

통신 요금 납부서

바둑이

1. 통신사 데이터 과금 방식



1. 통신사 데이터 과금 방식

만약 현재 과금 정책을 사용하지 않는다면 ?

통신 요금 납부서

철수

통신 요금 납부서

바둑이

1. 통신사 데이터 과금 방식

그렇다면 모든 나라에서 이러한 취약점이 존재할까?

논문에 따르면 아래 그림과 같이 국내 통신사는 TCP Restransmission에 대해 과금을 하지 않는 반면 해외 통신사 (AT&T,Verizon)등은 모든 패킷에 대해 과금 정책을 시행

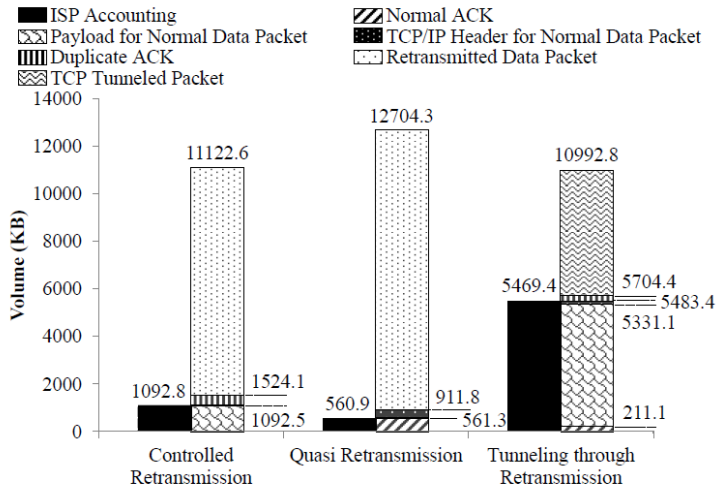


Figure 1: Experiment results of ISP-1 and 3

국내 통신사의 과금 시스템

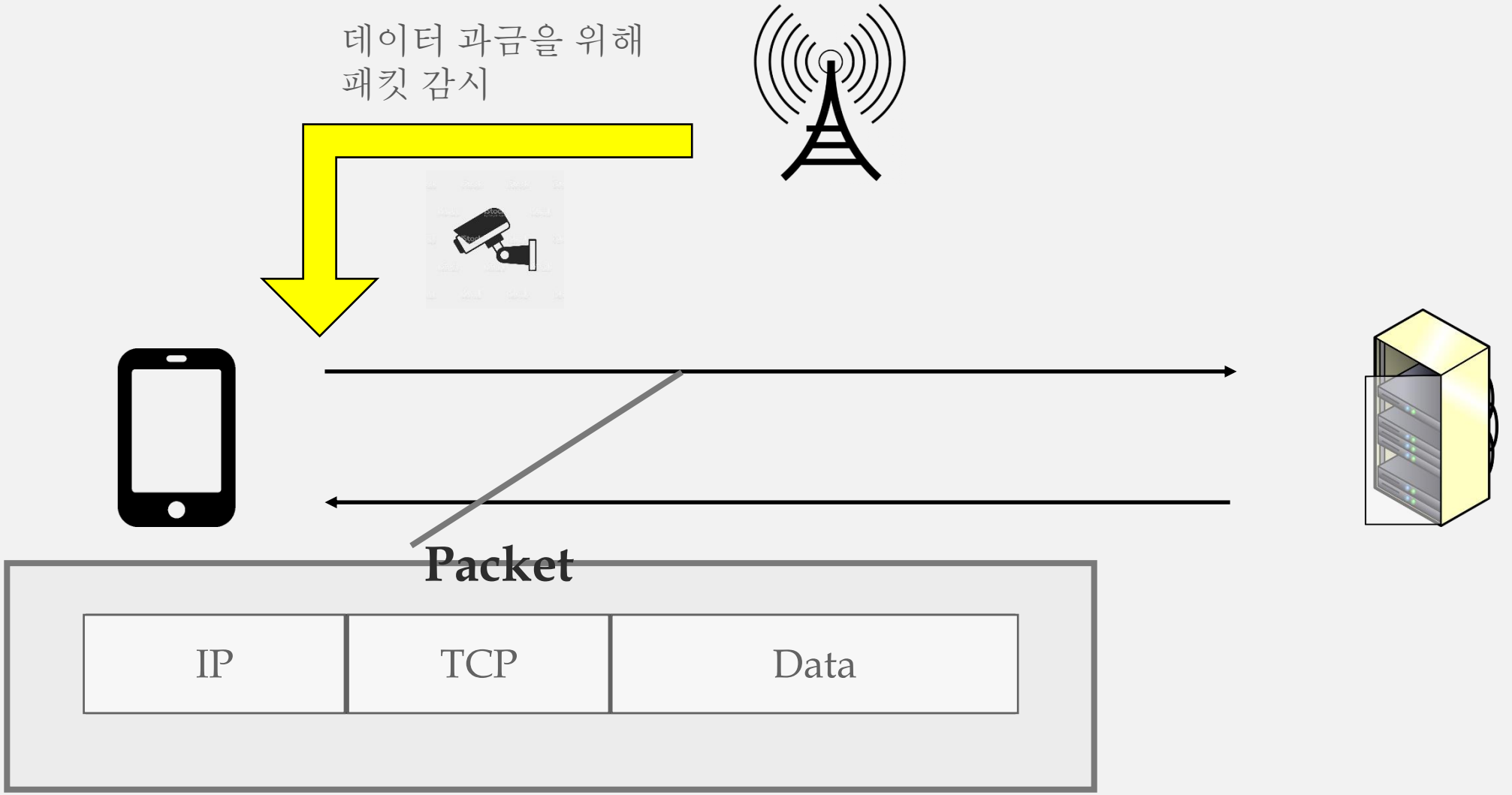
ISPs (Country)	Accounting Policy
AT&T, Verizon (U.S.)	All Packets
SKT, KT, LGU+ (South Korea)	Normal Packets

Table 1: Accounting policies for TCP retransmission

논문에서 언급한 해외 통신사의 과금 정책

프로그램 동작 원리

2. 프로그램 동작 원리



2. 프로그램 동작 원리

Src IP : Mobile IP

Dest IP : Tunneling Server IP

Seq Num : 1
Ack Num : 1
Src Port : User Choice
Dest Port : User Choice

데이터 과금을 위해 패킷 감시

Modified Packet

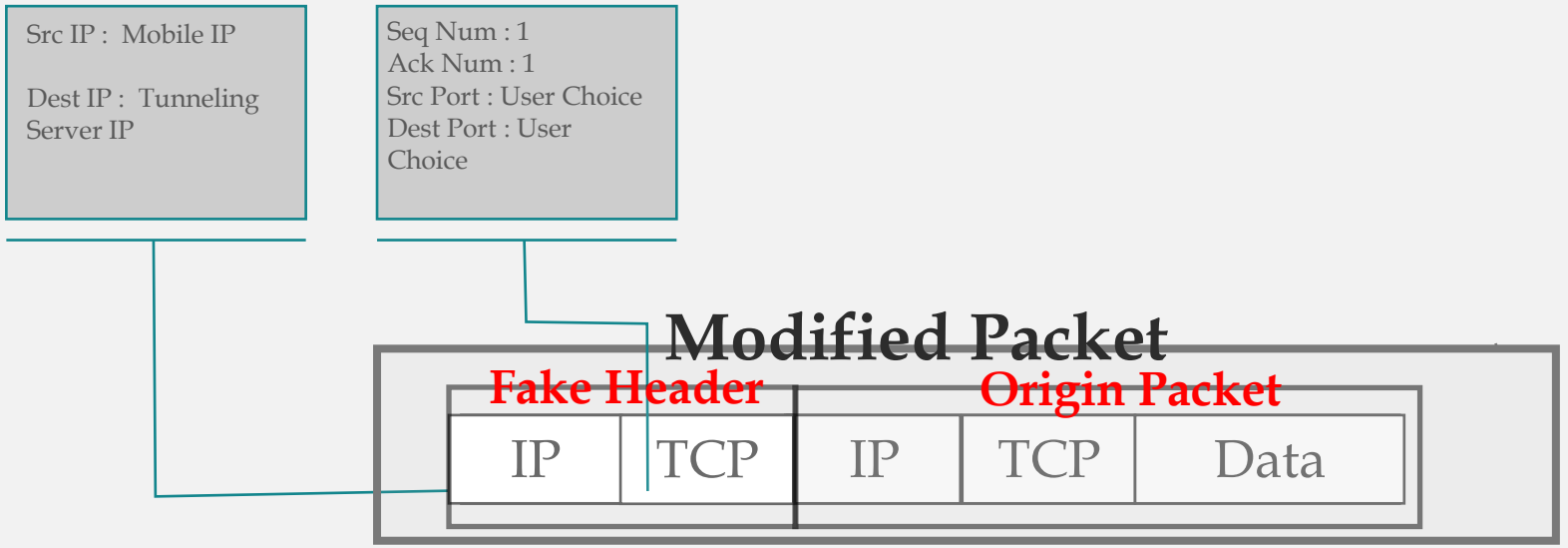
Fake Header | Origin Packet

IP	TCP	IP	TCP	Data

Origin Packet

IP	TCP	Data

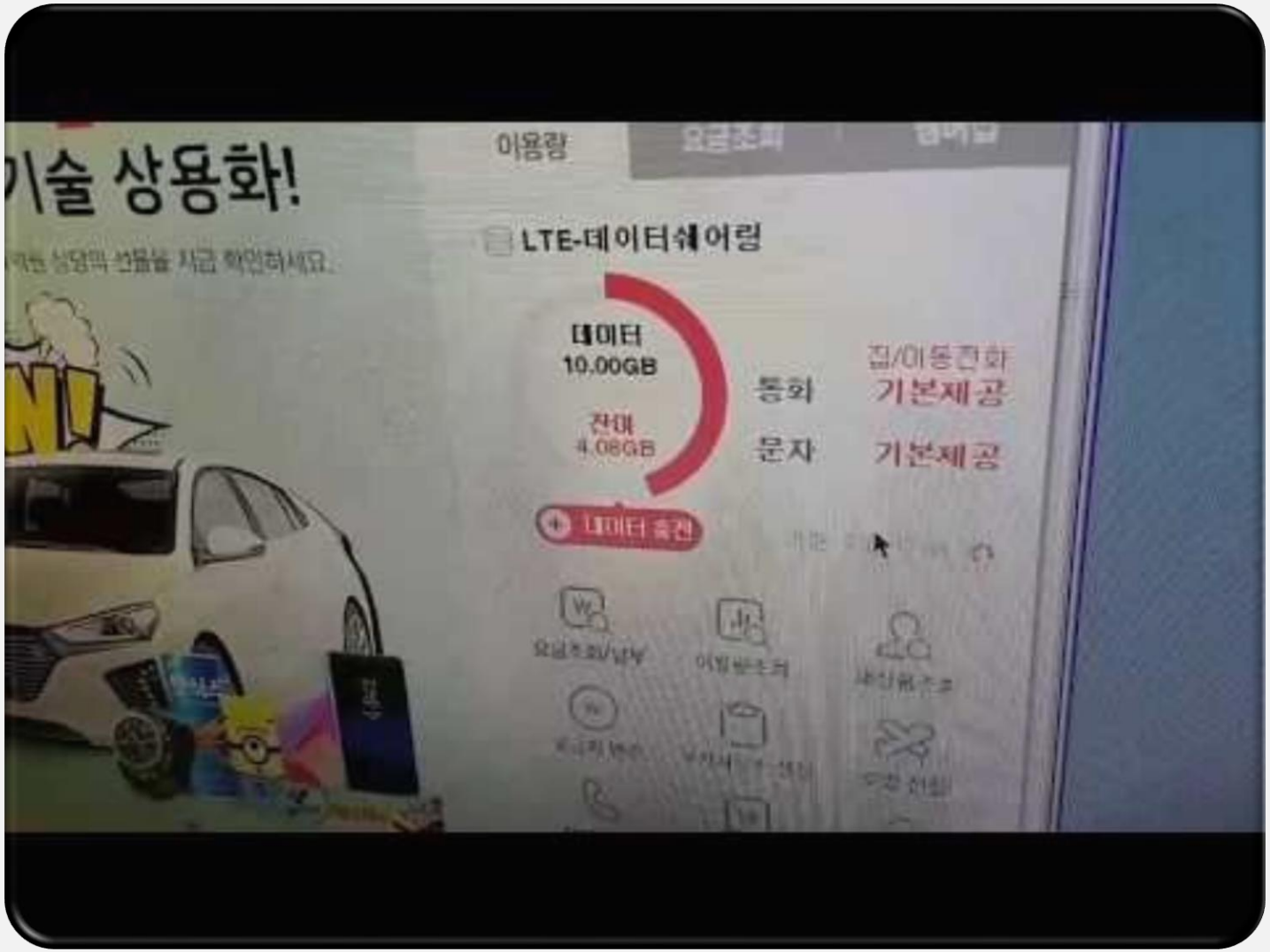
2. 프로그램 동작 원리



핸드폰은 실제로 서비스(Youtube, Naver 등)과 직접 통신을 하는 것 같지만 실제로는 Tunneling Server와 통신을 하고 있고, 통신사는 Server랑 통신하는 패킷의 내용으로 과금을 하기 때문에 과금 정책의 취약점을 이용해 데이터를 과금 없이 사용 가능

시연 영상

3. 시연 영상


기술 상용화!
이용량
LTE-데이터쉐어링
데이터
10.00GB
잔여
4.08GB
데이터 충전
통화
기본제공
문자
기본제공

향후 계획(취약점에 대한 패치)

4. 향후 계획

- 처음 이 취약점을 접했을 때는 이미 논문으로 발표된 상태
  ※논문 발표일 : 2013년
- 논문을 발표한 교수진(석,박사)들이 이미 해당 취약점에 대한 분석 시스템 및 보안 대책을 제출
- 비용이나 시스템 운영 문제로 인해 사실상 보안 대책 적용이 어려움
- 4년이 지난 지금 여전히 취약점이 존재(국내에서는 앞으로도 이러한 취약점이 존재 할 것으로 예상)

Q&A

Thanks To:
이경문 교수님 , 강진오 학생

아이콘 및 이미지 출처 : google.com
참고 학술 자료 : Impact of Malicious TCP Retransmission on Cellular Traffic Accounting