CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY

네트워크 취약점 분석 프로젝트 3종 세트

2018 CCIT 봄학기 프로젝트 발표회

CCIT 교육생 : 배대식 / 조현욱 / 조수홍 / 정현경 / 황선홍 / 표상영

발표자 : 표상영

CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

C C I T
프로젝트
발 표 회

교수님 소개

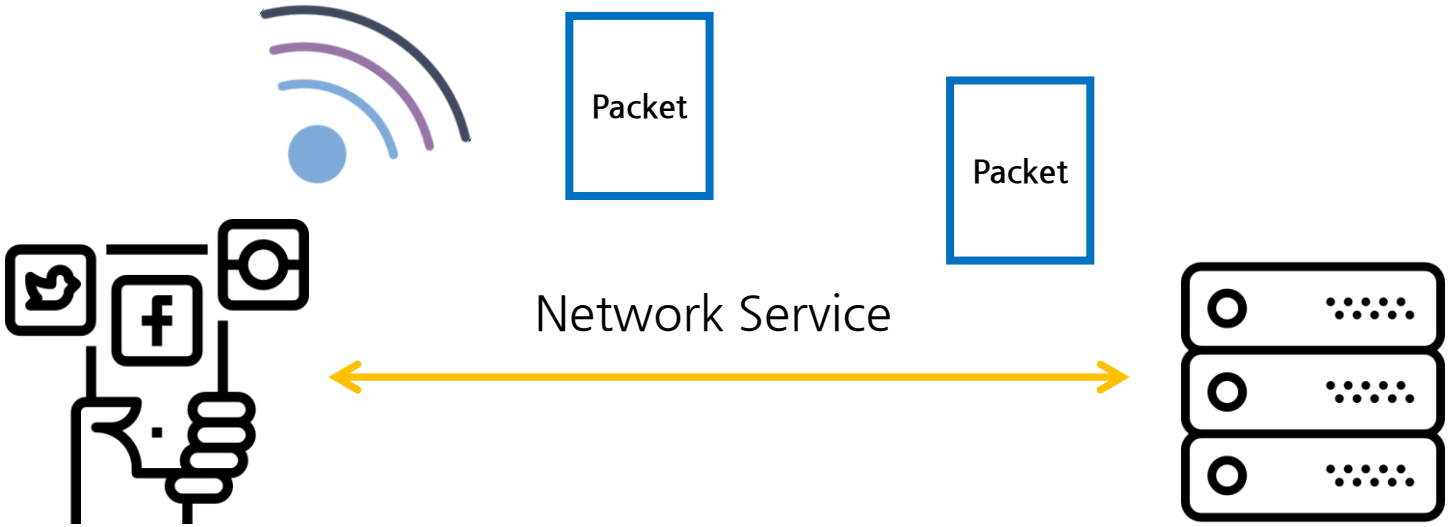
#이경문 교수님
Network Offensive & Defensive
한국정보기술연구원 'Best of the Best' Mentor
Homepage - gilgil.net

#윤종문 교수님
How to Interwork API with ESM
세코원 대표이사

#이병천 교수님
Project Support & Consulting
한국정보보호학회 이사
정보보호학회 논문지 편집위원

Table of contents

Bring_Your_Cookie



Bring_Your_Cookie

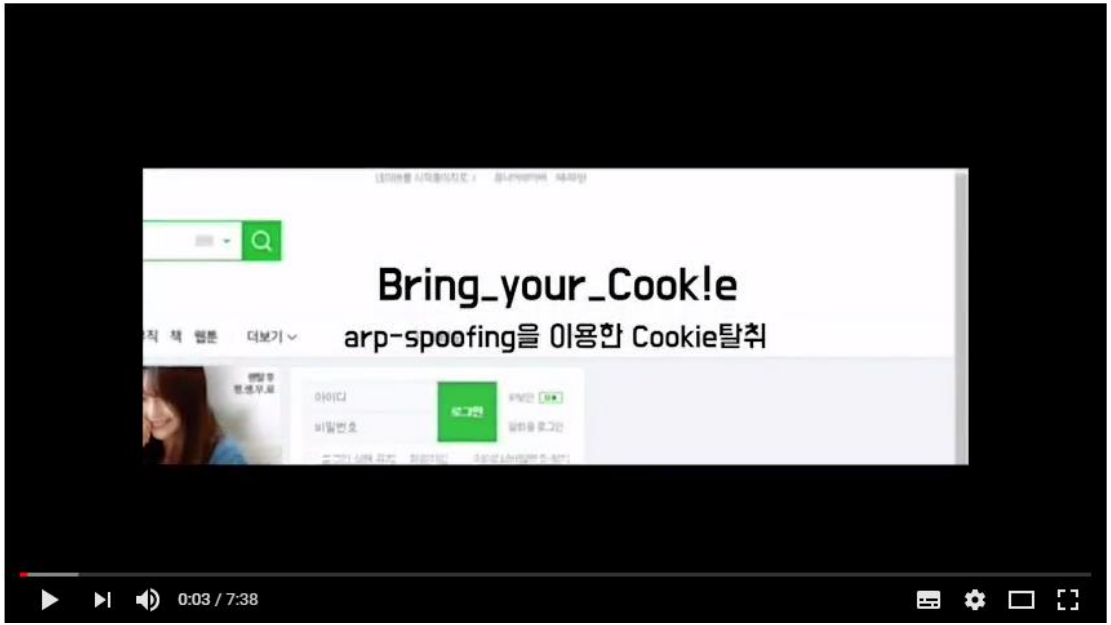
[Wireshark Tool]

591	14.884619	23.35.222.164	172.31.14.199	TCP	1440 443 → 49597 [ACK] Seq=44887 Ack=11922 Win=2397 Len=1386 [TCP segment of a reassembled PDU]
592	14.884620	23.35.222.164	172.31.14.199	TLSv1.2	379 Application Data
593	14.884872	172.31.14.199	23.35.222.164	TCP	54 49599 → 443 [ACK] Seq=11930 Ack=57779 Win=259 Len=0
594	14.886113	23.35.222.164	172.31.14.199	TCP	1440 443 → 49597 [ACK] Seq=46273 Ack=11922 Win=2397 Len=1386 [TCP segment of a reassembled PDU]
595	14.886289	172.31.14.199	23.35.222.164	TCP	54 49597 → 443 [ACK] Seq=11922 Ack=47659 Win=259 Len=0
596	14.886651	172.217.31.174	172.31.14.199	GQUIC	1392 Payload (Encrypted), PKN: 2
597	14.887349	172.217.31.174	172.31.14.199	GQUIC	73 Payload (Encrypted), PKN: 3
598	14.887350	23.35.222.107	172.31.14.199	TCP	60 443 → 50395 [ACK] Seq=147 Ack=569 Win=30336 Len=0
599	14.887930	23.35.222.164	172.31.14.199	TCP	1440 443 → 49597 [ACK] Seq=47659 Ack=11922 Win=2397 Len=1386 [TCP segment of a reassembled PDU]
600	14.888581	23.35.222.164	172.31.14.199	TCP	1440 443 → 49597 [ACK] Seq=49045 Ack=11922 Win=2397 Len=1386 [TCP segment of a reassembled PDU]
601	14.888583	23.35.222.164	172.31.14.199	TLSv1.2	982 Application Data
602	14.888676	172.31.14.199	23.35.222.164	TCP	54 49597 → 443 [ACK] Seq=11922 Ack=51359 Win=259 Len=0
603	14.888925	172.31.14.199	172.217.31.174	GQUIC	81 Payload (Encrypted), PKN: 2, CID: 12658952440016569473
604	14.889147	172.31.14.199	172.217.31.174	GQUIC	83 Payload (Encrypted), PKN: 3, CID: 12658952440016569473
605	14.890448	23.35.222.164	172.31.14.199	TCP	1440 443 → 49598 [ACK] Seq=45941 Ack=10090 Win=2776 Len=1386 [TCP segment of a reassembled PDU]
606	14.890450	23.35.222.164	172.31.14.199	TCP	1440 443 → 49598 [ACK] Seq=47327 Ack=10090 Win=2776 Len=1386 [TCP segment of a reassembled PDU]
607	14.890513	172.31.14.199	23.35.222.164	TCP	54 49598 → 443 [ACK] Seq=10090 Ack=48713 Win=259 Len=0
608	14.891161	23.35.222.164	172.31.14.199	TCP	1440 443 → 49598 [ACK] Seq=48713 Ack=10090 Win=2776 Len=1386 [TCP segment of a reassembled PDU]
609	14.892082	23.35.222.164	172.31.14.199	TLSv1.2	1236 Application Data
610	14.892117	172.31.14.199	23.35.222.164	TCP	54 49598 → 443 [ACK] Seq=10090 Ack=51281 Win=259 Len=0
611	14.893552	172.31.14.199	23.35.222.164	TLSv1.2	972 Application Data
612	14.894613	172.31.14.199	23.35.222.164	TLSv1.2	972 Application Data
613	14.895883	172.31.14.199	23.35.222.164	TLSv1.2	970 Application Data

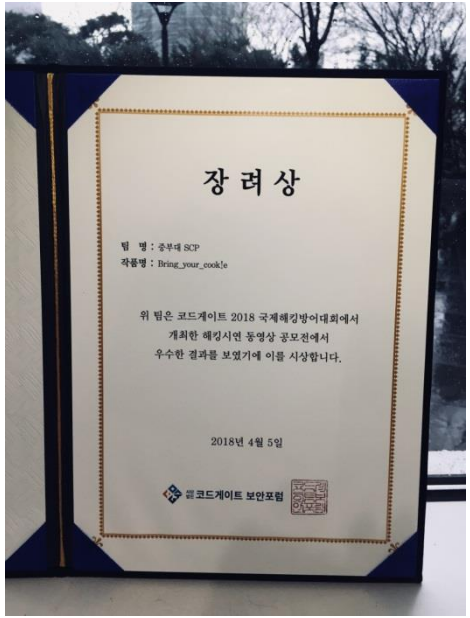
Sniffing된 무선 패킷들

Bring_Your_Cookie

캡쳐된 Packet에서 NAVER 로그인에 필요한 Cookie값 추출



Bring_Your_Cookie



Codegate2018 해킹시연 공모전 장려상(3위)
[황선홍,정재훈,표상영]

Drone hacking with Deauthentication Attack

#Deauthentication Packet
- 무선AP에 접속된 기기가 접속을 끊을 때 발생되는 패킷

#문제점
- Deauthentication Packet 송신자가 누구인지 확인하지 않고 받아들인다.

Drone hacking with Deauthentication Attack

시연영상

Drone hacking with Deauthentication Attack

[After Project..]

- SecurityPlus SUA 세미나 발표

- 대학정보보안동아리연합회 KUCIS 발표 예정

Preventing carrier data billing through packet manipulation

#통신사 데이터 과금 방식

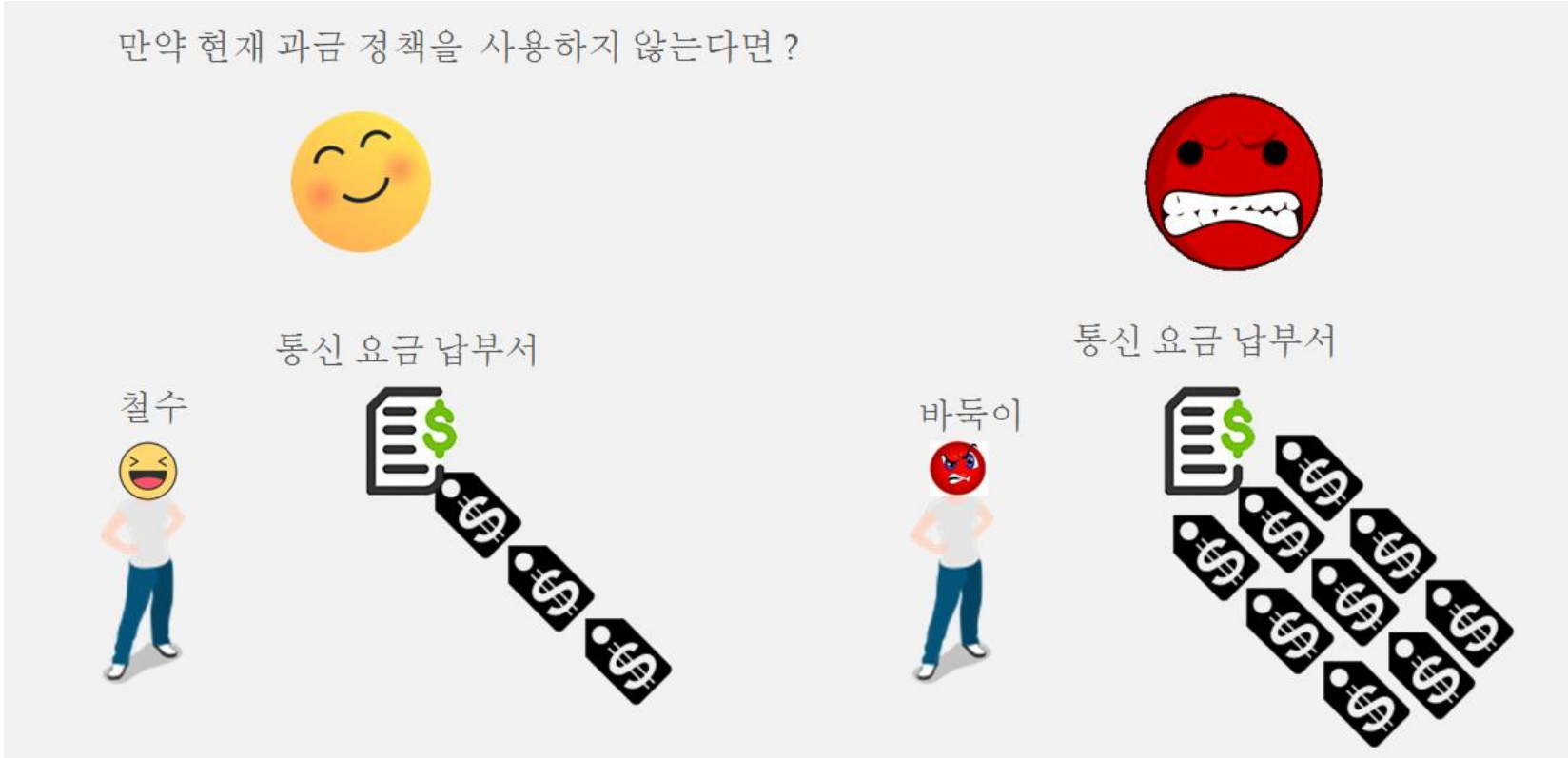
- UDP 통신 외 기타 프로토콜
  - 송 수신된 패킷의 데이터 길이를 측정하여 길이만큼 데이터 과금

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

Preventing carrier data billing through packet manipulation

Preventing carrier data billing through packet manipulation



Preventing carrier data billing through packet manipulation

시연영상

Best of the Best(BoB)

- 한국정보기술연구원 (KITRI) 차세대 보안리더 양성 프로그램
- 교육생 총 160명
- 매 년 약 1200명 가량 지원

Best of the Best(BoB)

교육생 지원 및 특전

공통지원사항


교육생 전용
학습공간


최신 IT 기기
참고서적


교통비 지원
수강료 무료


프로젝트 활동지원


지방 교육생을 위한
기숙사 지원

정보보안
영어회화 교육

수료자 특전


- 사후보안 연구모임


- 맞춤형 진로연계

인증자 특전


- 미래창조과학부 인증서
- KITR 인증서

- **Best 10**
  - 1,000만원 상당의 사후관리 및 진로지원
  - 국외연수
- **그랑프리**
  - 창업 및 기술사업화 지원

Best of the Best(BoB)

사후관리

리크루팅 전문가 네트워크, 잡페어 등을 통한 교류의 장 지원

린(Lean) 스타트업, 창업보육 등 기술 중심의 창업이 가능하도록 현실적 지원방안 추가마련 (무료 컨설팅 지원사업 등)

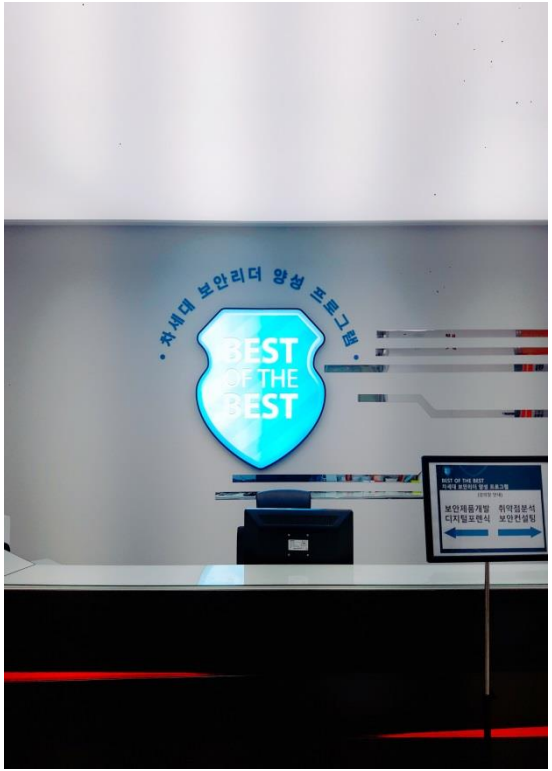
대학과의 MOU를 통한 직접적인 연계방안 추진

수료생 사후관리 시스템

구분	수행내용
연구개발 지원	우수 연구인력 발굴 및 연구분야 진로진출 지원
경진대회팀	국제 정보보안 경진대회 출전을 통한 글로벌 최신 기술 동향 습득
취약점 분석팀	산업계와의 공동 프로젝트 추진을 통한 취업/창업 지원
보안컨설팅팀	소기업 중 취약계층 무료 취약점 분석
정기교류모임	다양한 보안정보 공유 및 의사소통 등 인적 네트워킹 형성
재능기부	중학교, 고등학교, 대학교, 동아리 방문교육 및 세미나 등을 통한 정보보안 기술 전파
운영기반 시스템	수료생 관리 및 관련 기술정보 공유를 위한 운영기반 제공

Best of the Best(BoB)

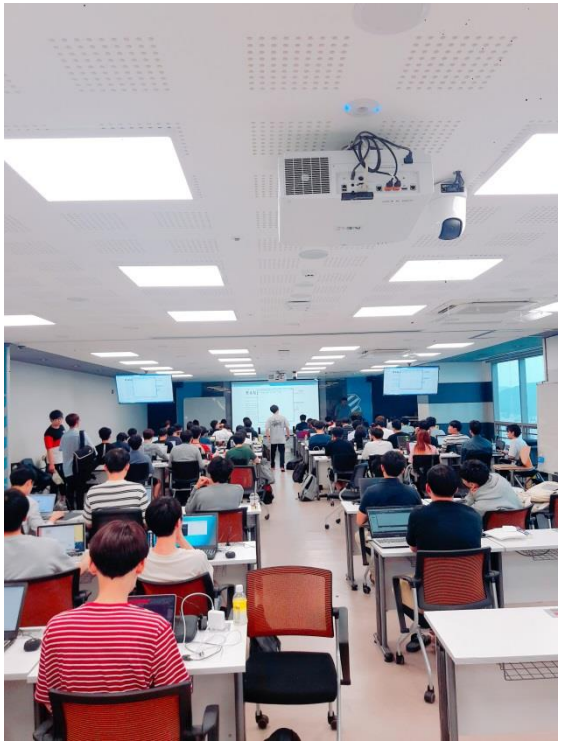
건물 외부



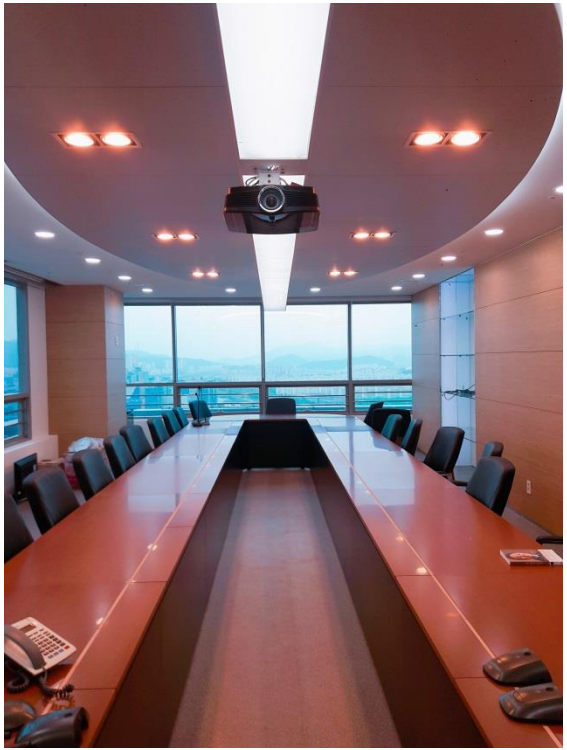
로비 카운터

Symbol

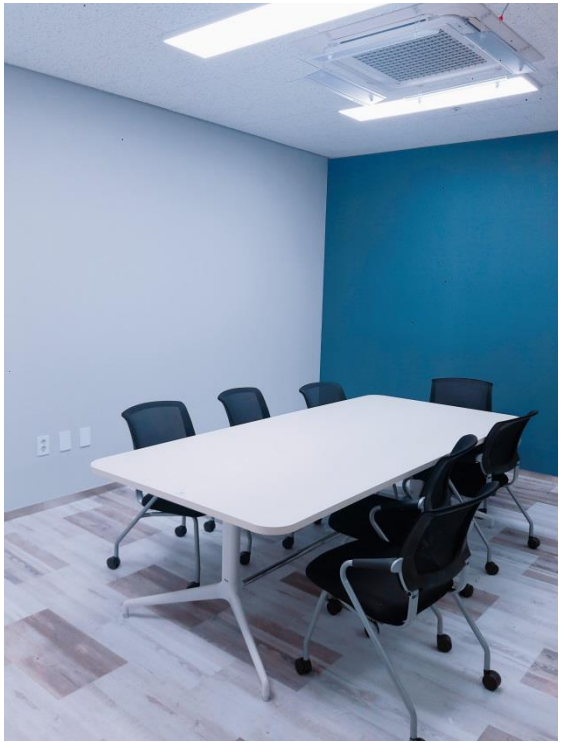
Best of the Best(BoB)



강의실



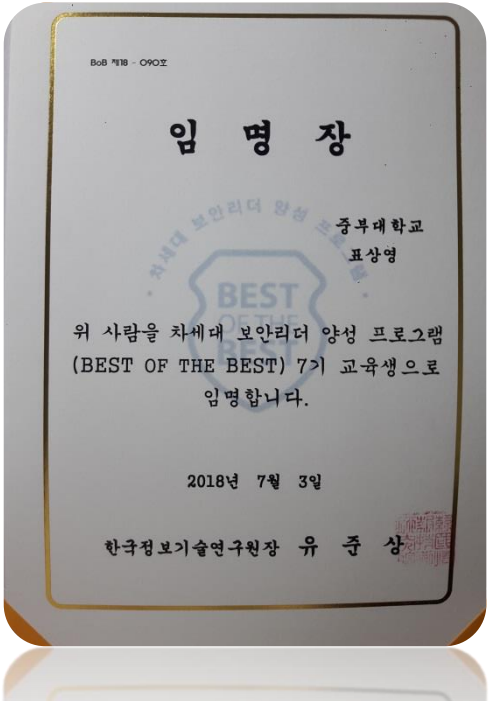
대회의실



멘토링 룸

Best of the Best(BoB)

CCIT 프로그램에서 교수님들께 차별화된 교육을 받고 다양한 경험을 쌓았으며
그 결과, 중부대 정보보호학과 합격자 6명(**장한빈, 정영호, 이경수, 손현수, 조현욱, 표상영**) 중
CCIT 교육생 5명 (**장한빈 , 정영호 , 이경수 , 조현욱 , 표상영**) BoB 최종합격!


BoB 제18 - 090호

임 명 장

중부대학교
표상영

위 사람을 차세대 보안리더 양성 프로그램
(BEST OF THE BEST) 7기 교육생으로
임명합니다.

2018년 7월 3일

한국정보기술연구원장 유 준 상

감사합니다.