

제53회
2020 온라인 춘계학술발표대회

신진학자 워크숍

Hardware-Based Techniques for Memory Safety

조영필 교수
(한양대학교)



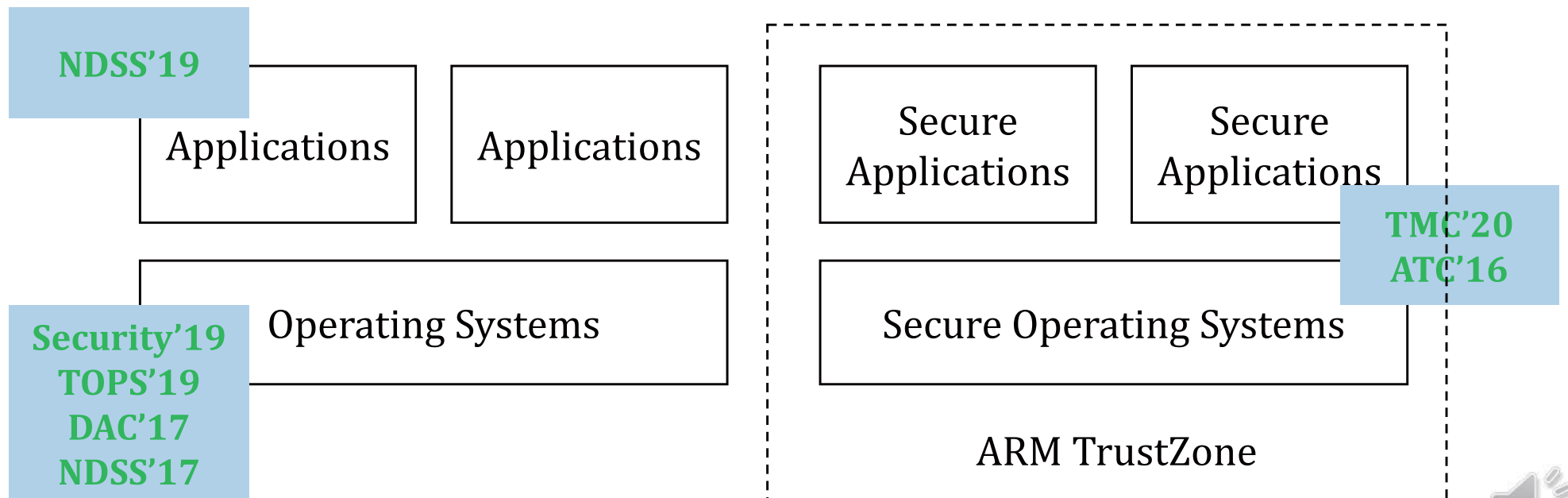
Hardware-Based Techniques for Memory Safety

조영필

한양대학교

Who am I

- 조영필 (Yeongpil Cho)
 - B.S. POSTECH, EE
 - Ph.D. Seoul National University, ECE
 - Before Soongsil University, Software
 - Now Hanyang University, CS



Bounds comparison

- **Intel MPX** (Memory Protection eXtensions)

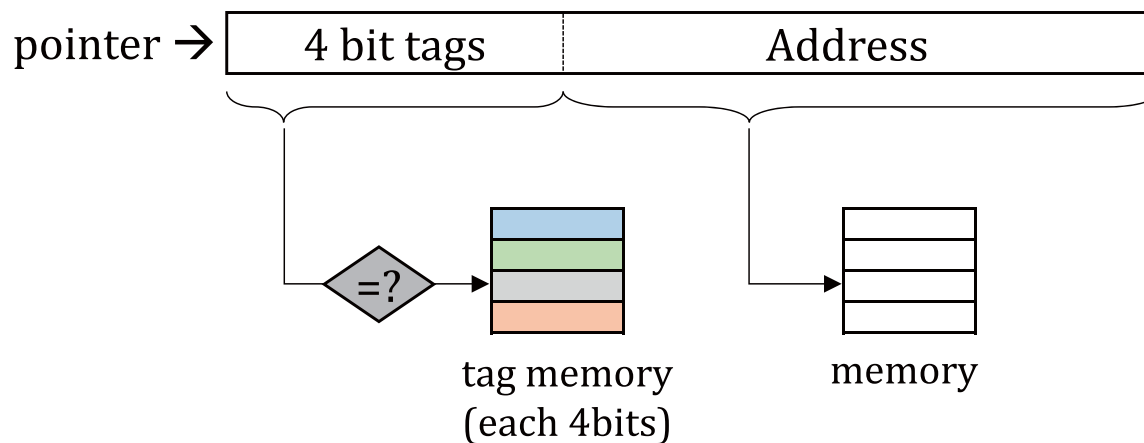
- Pointer-level bounds comparison
- Hardware-assisted per-pointer bounds managements and checks
 - Trie-structured bounds table
 - four bounds registers
- Recent work
 - BOGO: buy spatial memory safety, get temporal memory safety (almost) free, ASPLOS 2019

```
void init() {  
    char A[10];  
    char B[20];  
    bnd0 = bndmk A, A+10  
    bndstx A, bnd0  
    ...  
    strcpy (A, B, 10);  
}  
  
void strcpy (char *dest, char *src) {  
    bndldx bnd0, dest  
    bndldx bnd1, src  
    while (*src != '\0') {  
        bndcl bnd0, dest  
        bndcu bnd0, dest  
        bndcl bnd1, src  
        bndcu bnd1, src  
        *dest++ = *src++;  
    }  
}
```

Tag comparison

- **ARM MTE (Memory Tagging Extension)**

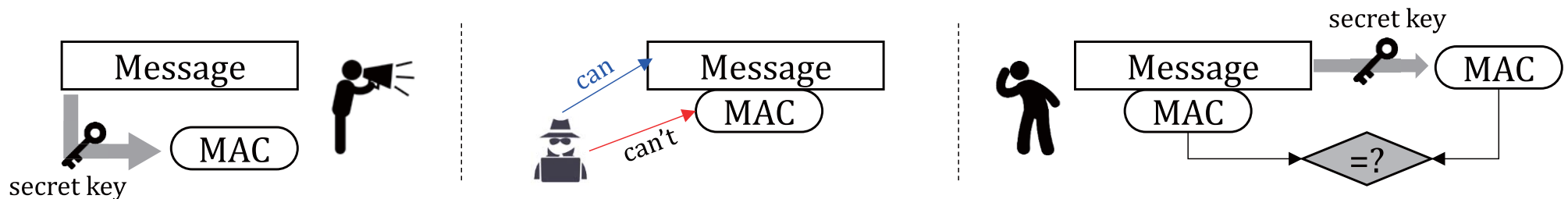
- Pointers are allowed to access the memory with the matching tag
- Hardware-assisted efficient tag management
- Recent work
 - Memory Tagging and how it improves C/C++ memory safety, Report



```
void init() {  
    char A[10];  
    char B[20];  
    irg A, A  
    for (i=0; i<10; i++)  
        stg A[i];  
    irg B, B  
    for (i=0; i<10; i++)  
        stg A[i];  
    ...  
    strcpy (A, B, 10);}  
  
void strcpy (char *dest, char *src) {  
    while (*src != '\0') {  
        *dest++ = *src++;  
    }  
}
```

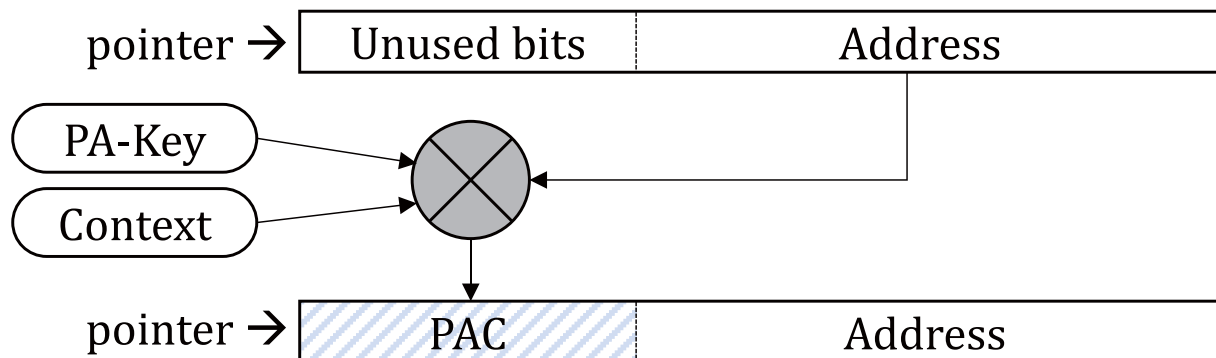
Pointer protection

- MAC (Message Authentication Code)



- **ARM PA (Pointer Authentication)**

- Attaches PAC (Pointer Authentication Code) to a pointer
- Recent work
 - PAC it up: Towards Pointer Integrity using ARM Pointer Authentication



```

pacia lr, sp      } prologue
push lr

...
blr ...            } body
...

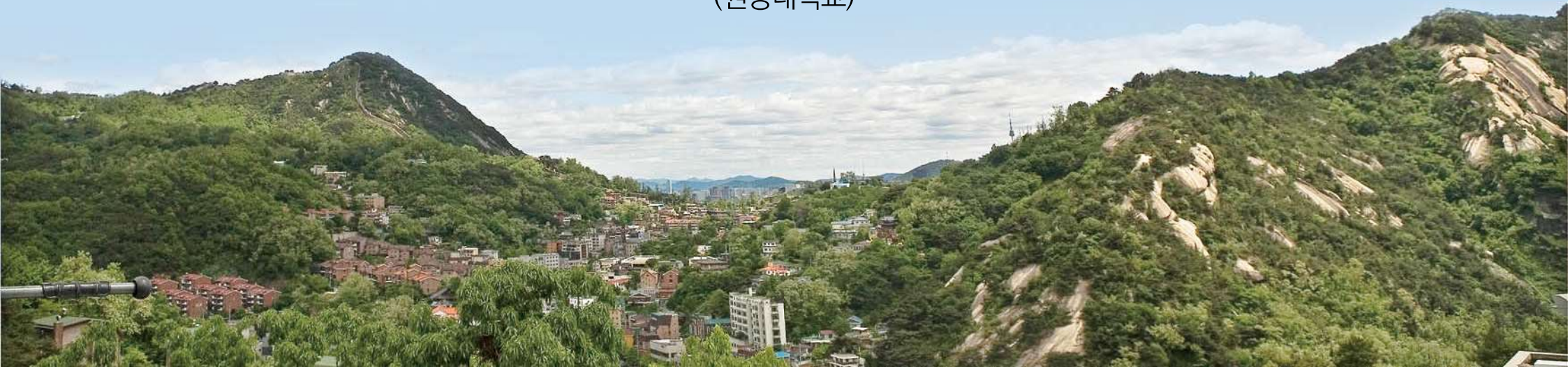
pop lr
autia lr, sp      } epilogue
ret lr
    
```


제53회
2020 온라인 춘계학술발표대회

신진학자 워크숍

비대면 혼합현실(MR) Tele-Conference 시스템 연구 현황

조동식 교수
(원광대학교)



비대면 혼합현실(MR) Tele-conference 시스템 연구 현황

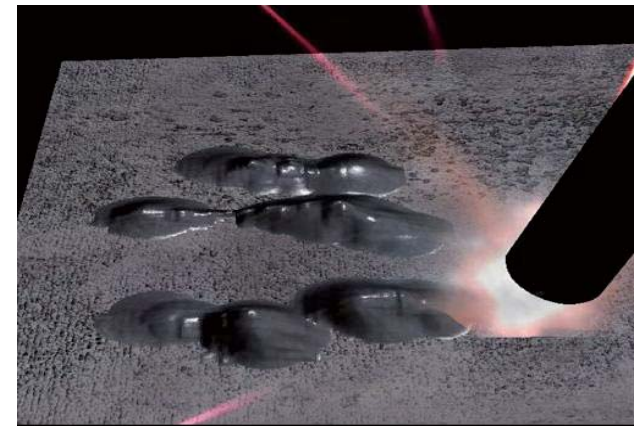
Dongsik Jo (조동식)

원광대학교 디지털콘텐츠공학과

dongsik1005@wku.ac.kr

발표자 소개

- 2003 ~ 2004: 한국해양과학기술원 연구원 (과학적 가시화 연구 수행)
- 2004 ~ 2017: 한국전자통신연구원(ETRI) VR/AR 연구그룹
VR/AR 프로젝트 15년 동안 수행
 - VR 훈련 시뮬레이션 시스템 (예. 용접 훈련 시스템)
 - 엔터테인먼트 VR 시스템 (예. 가상 사파리 체험 시스템)
- 가상현실/증강현실의 미래 공동 저자 (2018년 출판)
- 2018 ~ : 원광대학교 디지털콘텐츠공학과
- 2019 ~ : 컴퓨터그래픽스 학회 (KCGS) 조직 위원
- 2019~ : 원광대학교 SW중심대학 산업지원 센터장



Motivation: Tele-conference

2D

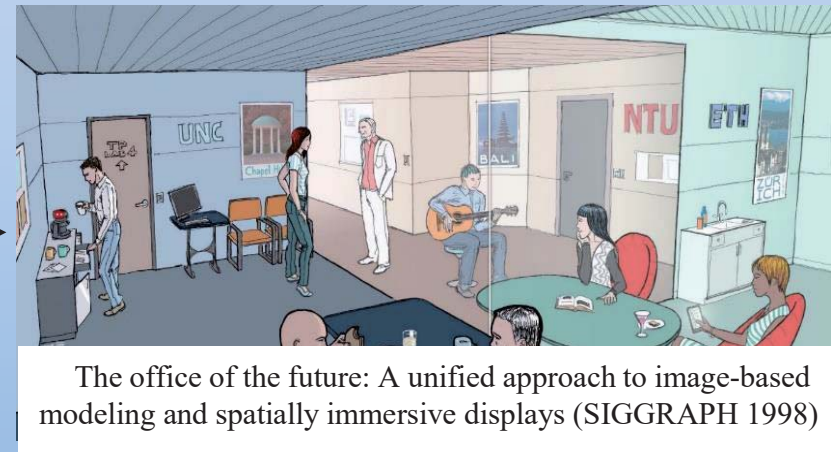


공간에
투영된
느낌 제공



사용자
이동이
자유로움

3D



혼합현실 (MR) 가상 아바타



Mixed reality teleconference (from The Kingsman)

Motivation: MR Teleported Avatars



- ✓ 실제 사용자 공간에 Teleported Avatar 투영
- ✓ 원격지 사용자가 함께 존재하는 듯한 느낌을 제공

Motivation: MR Teleported Avatars

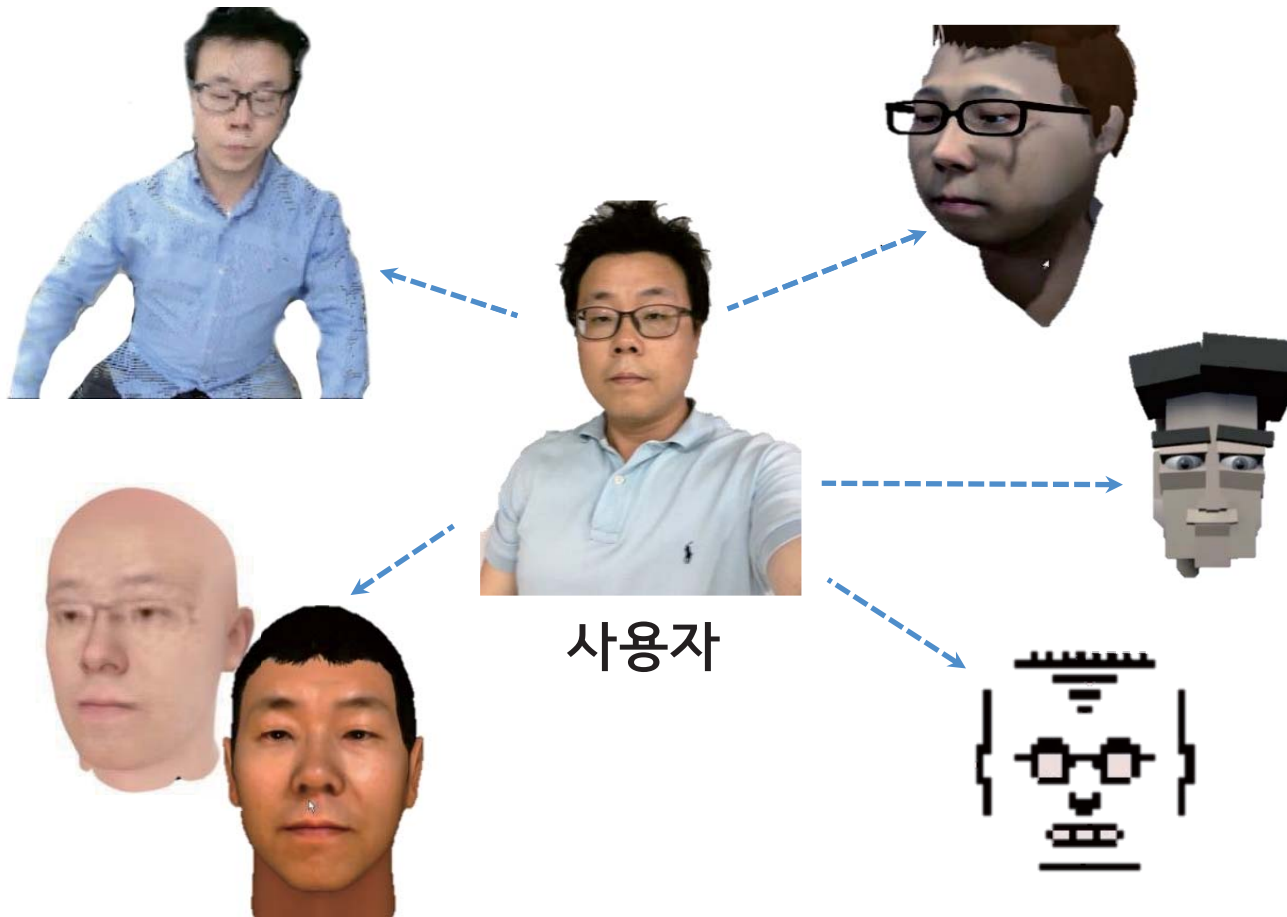


Facebook : 어떻게 하면 MR환경에서 Teleported Avatar와 공유된 경험 Level을 높일 수 있을까?

Motivation

MR Teleported Avatar 이슈 1

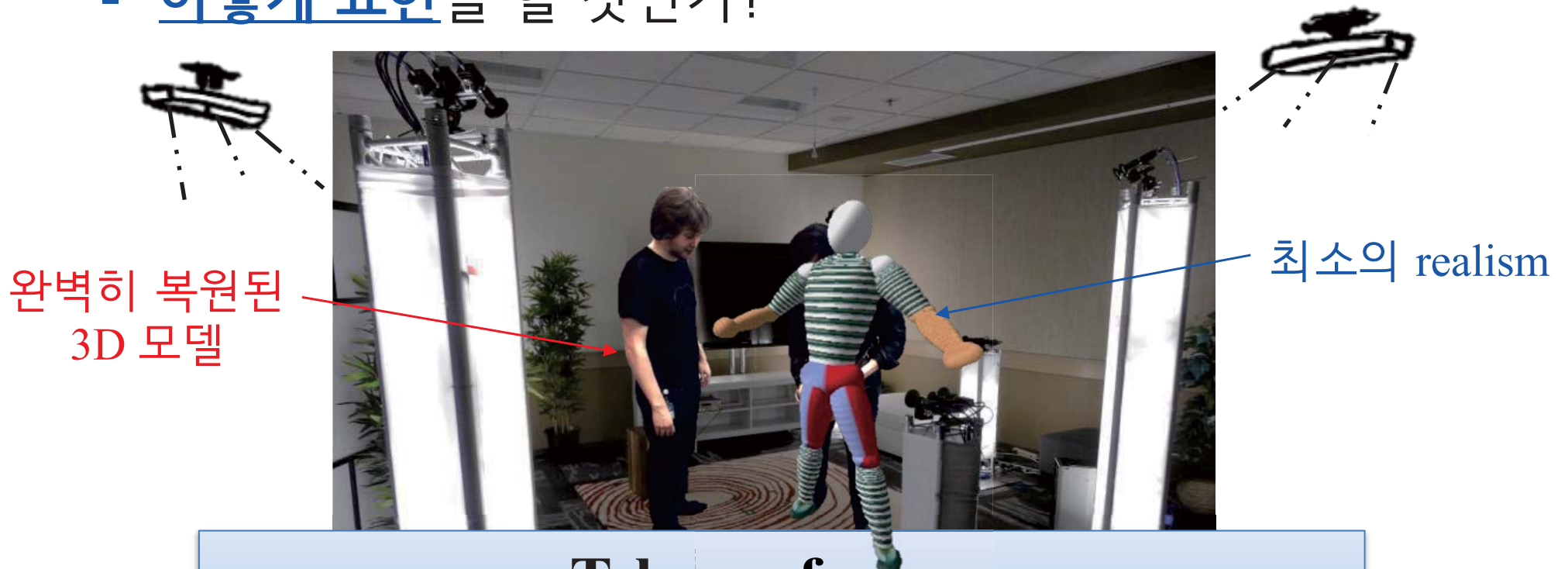
- 어떻게 표현을 할 것인가?



Motivation

MR Teleported Avatar 이슈 1

- 어떻게 표현을 할 것인가?



Tele-conference

- ✓ 항상 High-quality의 3D 모델로 복원하여 사용한다면?
 - 복잡한 시스템 구성, 컴퓨팅/네트워킹 리소스의 한계

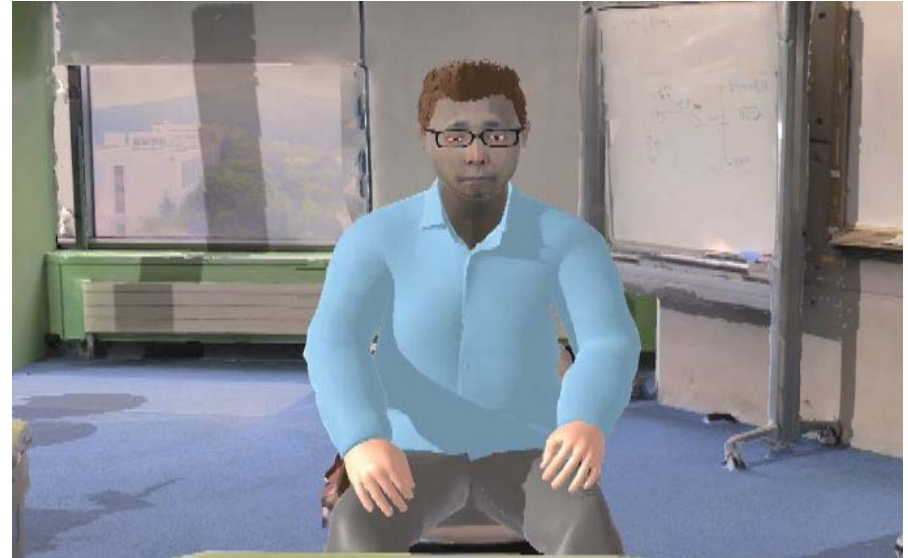
Motivation

MR Teleported Avatar 이슈 2

- 어디에 위치시킬 것인가?



Visual Form



Experiments

- **Experiment 1. Avatar's Visual Form : Co-presence 비교 분석**

- ✓ 아바타의 외형/배경 형태 Co-presence 비교



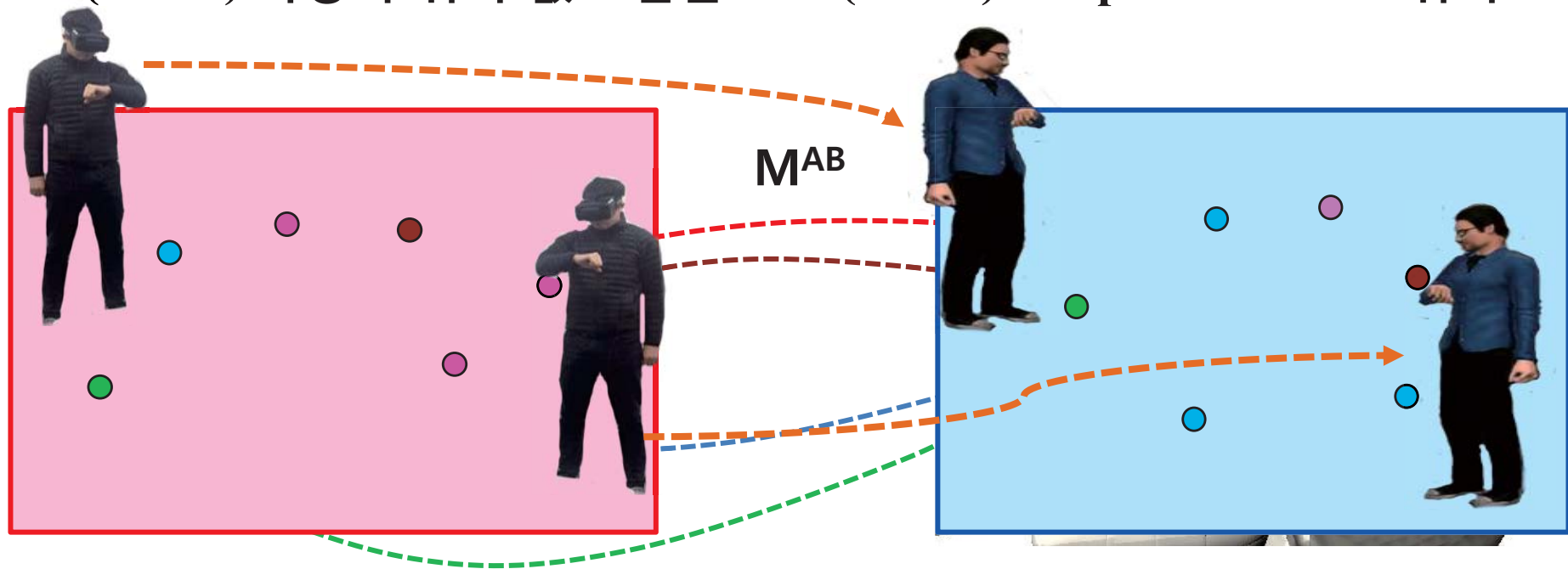
- **Experiment 2. Avatar's Visual Form : Trust 비교 분석**

- ✓ 아바타의 외형/배경 형태 Trust 비교



Teleported Avatar 위치 결정

- 매칭 결과 → 공간 간 변환 관계 (M^R) 설정
 - ✓ Least Square Approximation : $\text{Site_A} \cdot M^{AB} \approx \text{Site_B}$,
 $M^{AB} = (\text{Site_A}^T \cdot \text{Site_A})^{-1} \cdot \text{Site_A}^T \cdot \text{Site_B}$
- (Site A) 사용자 위치 값 * 변환 $M =$ (Site B) Teleported Avatar 위치



- ✓ 아바타-의자 간 충돌 처리: Navigation 영역 미리 설정, 충돌 회피

실시간 Teleported Avatar 위치/자세 Adaptation

- Local 영역 서로 다른 모양의 의자가 있는 경우
 - ✓ 예. 높이가 다른 의자
- 아바타의 위치/자세를 어떻게 맞추는 것인가?

Site A



Site B



실시간 Teleported Avatar 위치/자세 Adaptation

- 물체 (의자) 의 Key points 기반 Avatar Joint Positions 제어



Summary: Avatar's Environment Adaptation

■ 원격지의 서로 다른 환경

- ✓ 원격지 환경 간 상관관계 매칭
- ✓ Teleported Avatar의 위치 결정

■ 서로 다른 형태 (의자 높이) 물체

- ✓ 물체의 Key points를 기반으로 상관관계 설정
- ✓ 실시간 Tracking 적용한 Teleported Avatar 위치/자세 결정

ARIoT: 사용자 주변 사물과 연결된 증강현실

Future Trend

Augmented Reality

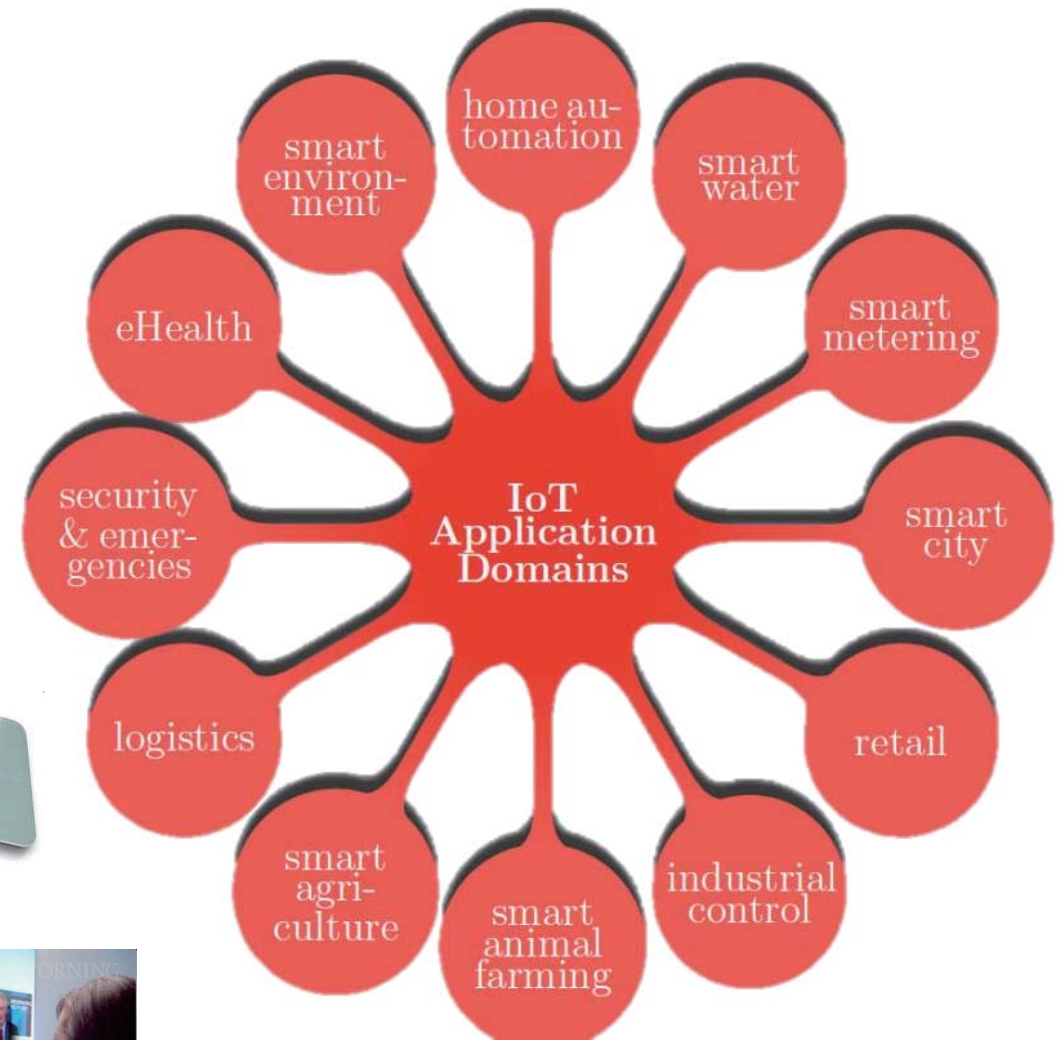
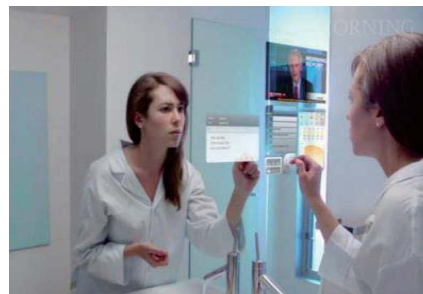


a live direct or indirect view of a physical, real-world environment whose elements are *augmented* (or supplemented) by computer-generated sensory input

Future Trend

IoT (Internet of Things)

*"from **anytime, any place** connectivity for **anyone**, we will now have **connectivity** for **anything**" - ITU (2005)*

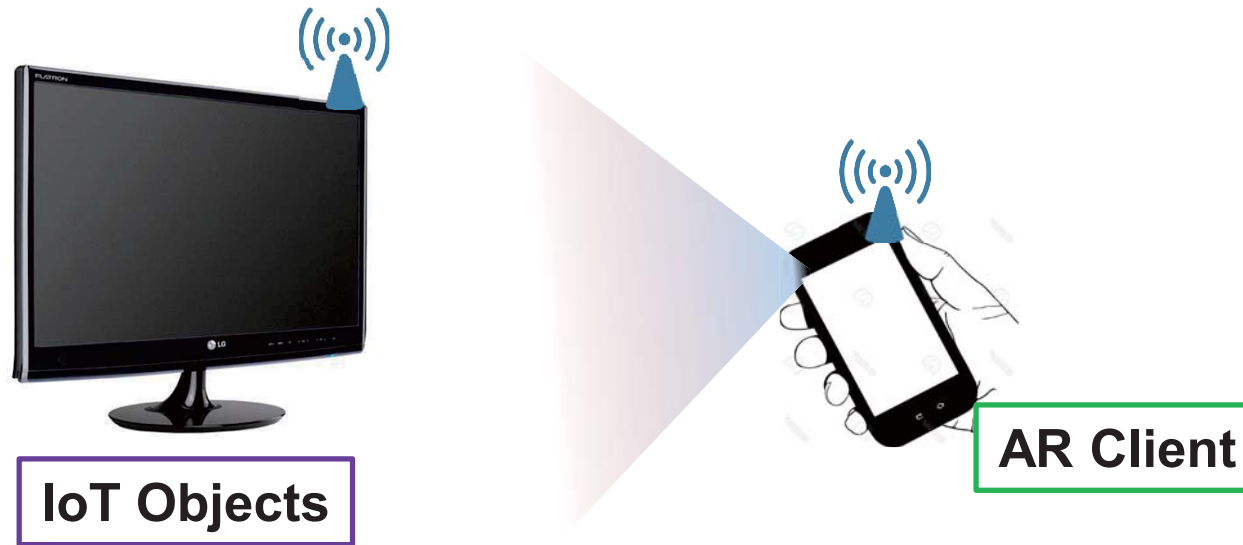


Approach



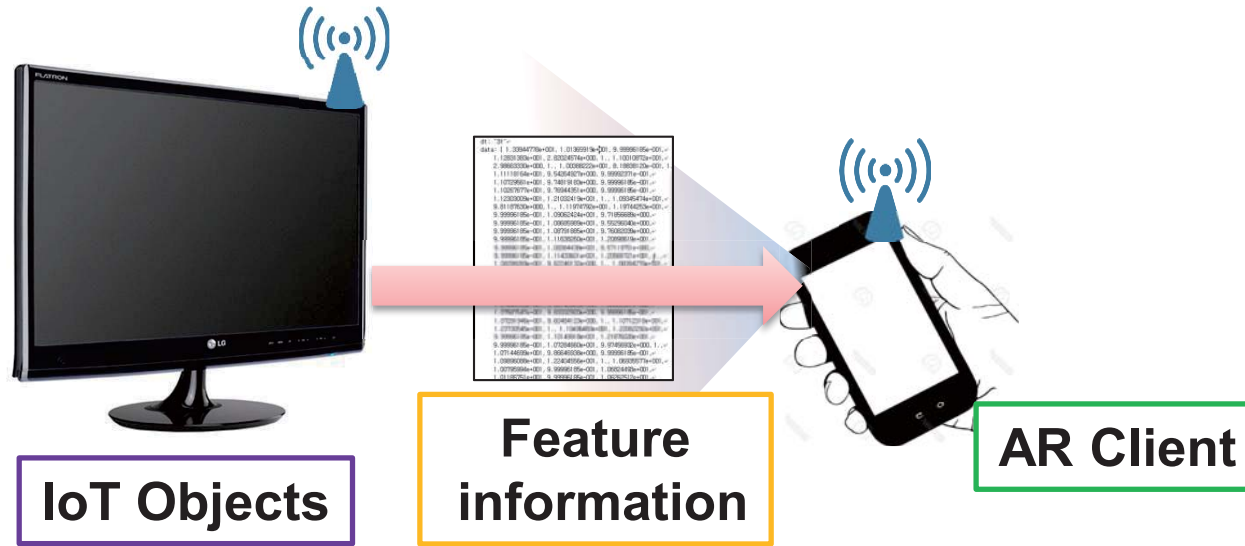
IoT Objects

Approach



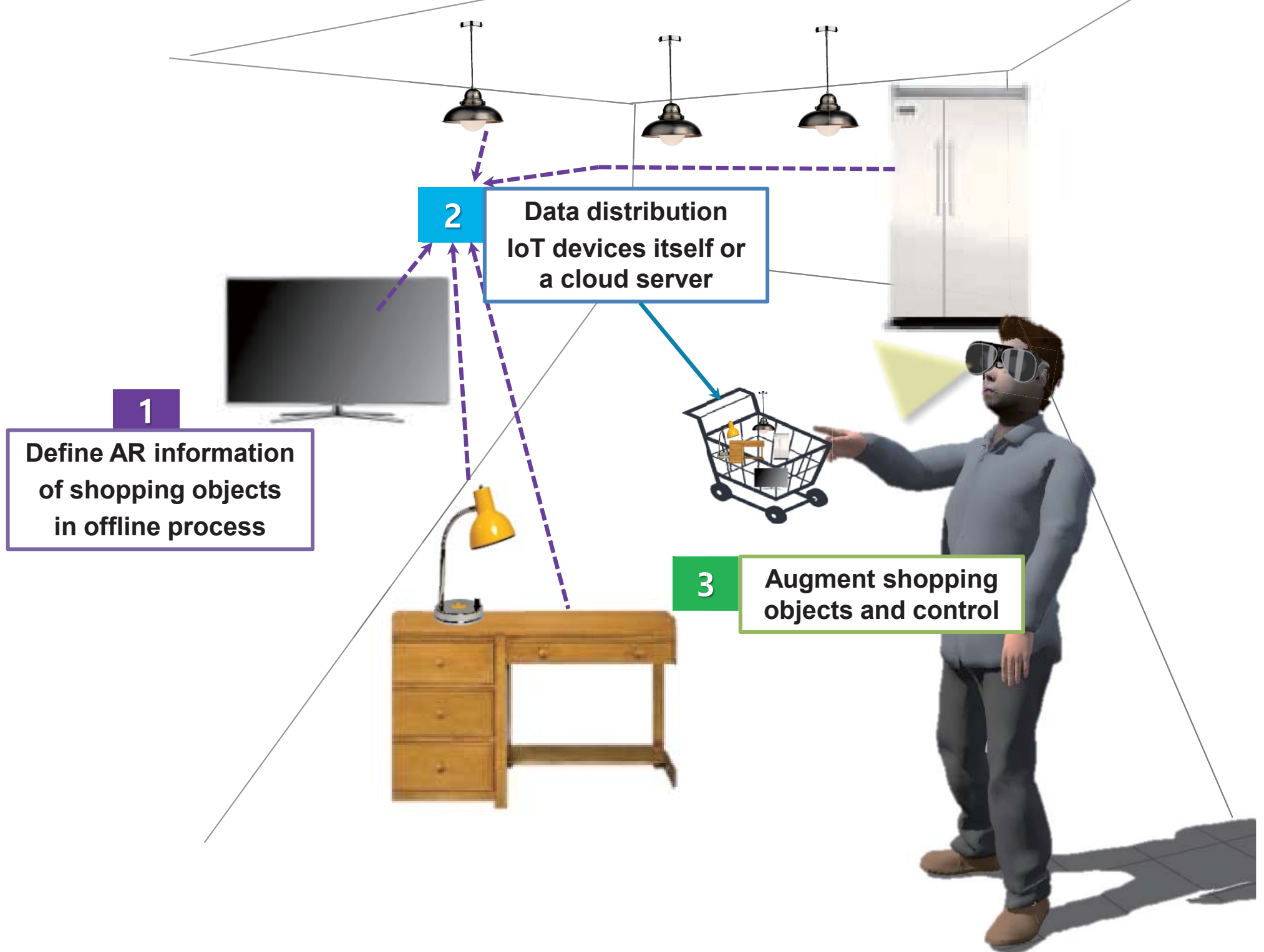
A mobile AR client select and connect to IoT objects in a given space

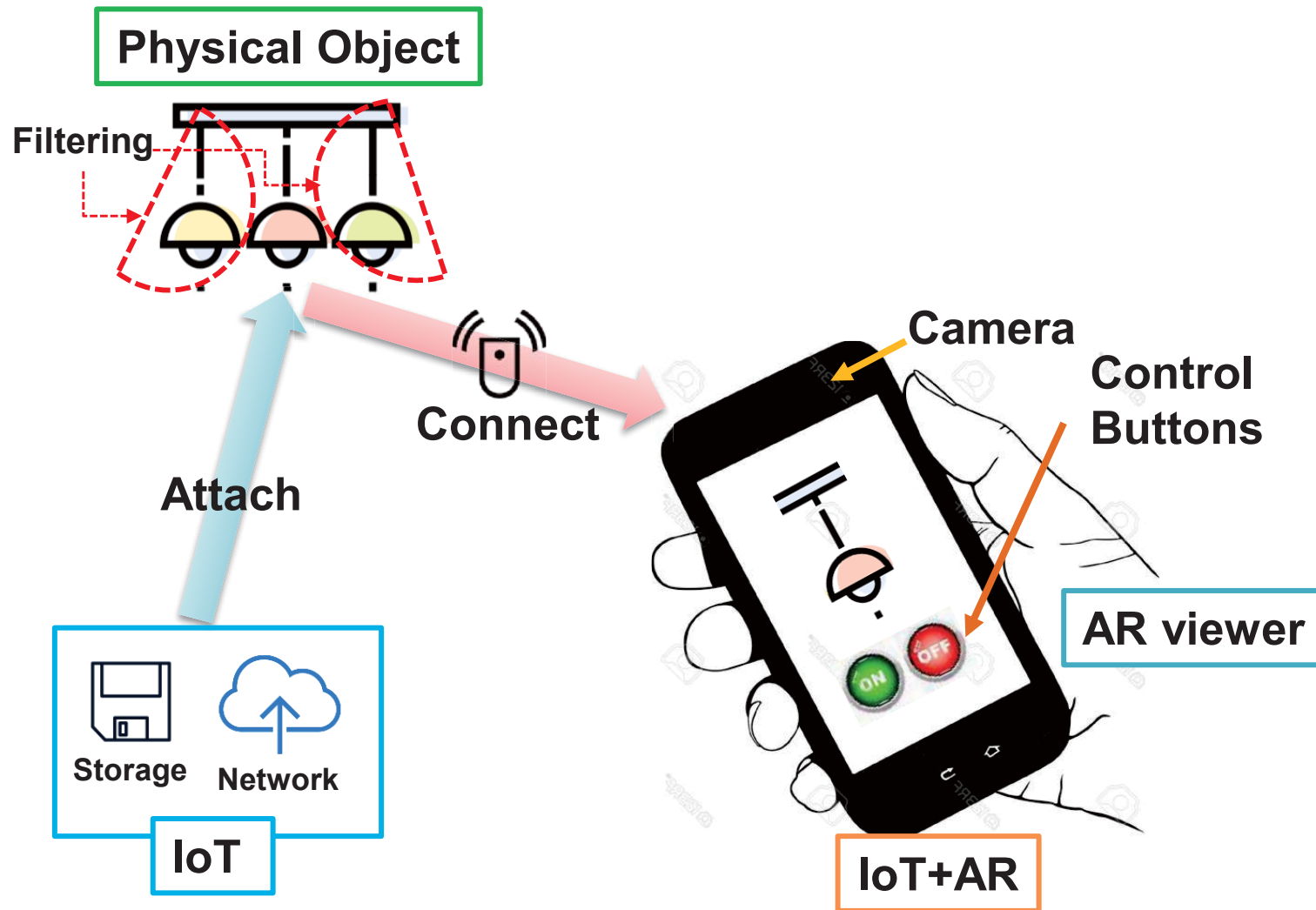
Approach



The IoT objects would provide feature descriptors and interactive augmentation contents for the AR client



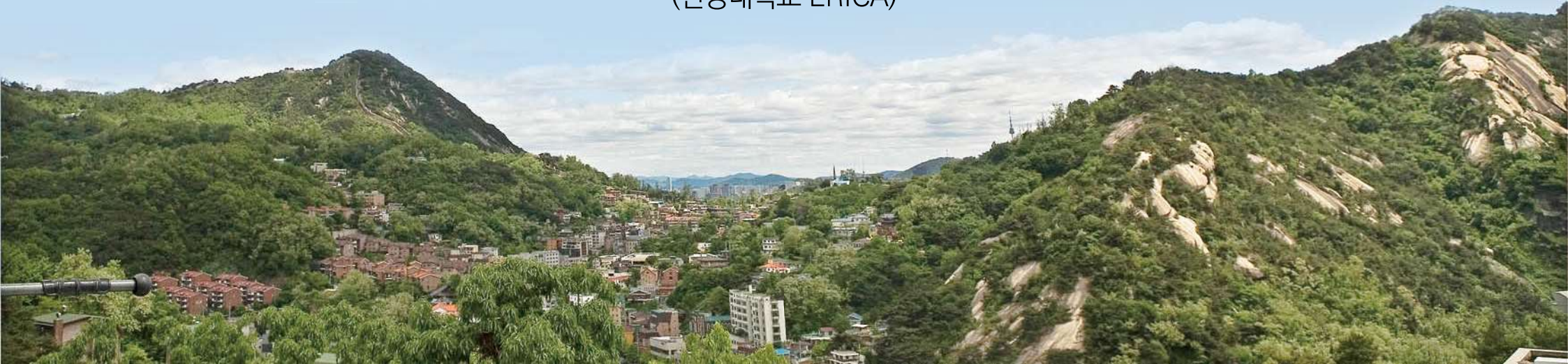




신진학자 워크숍

Understanding iOS-based Crowdturfing Through Hidden UI Analysis

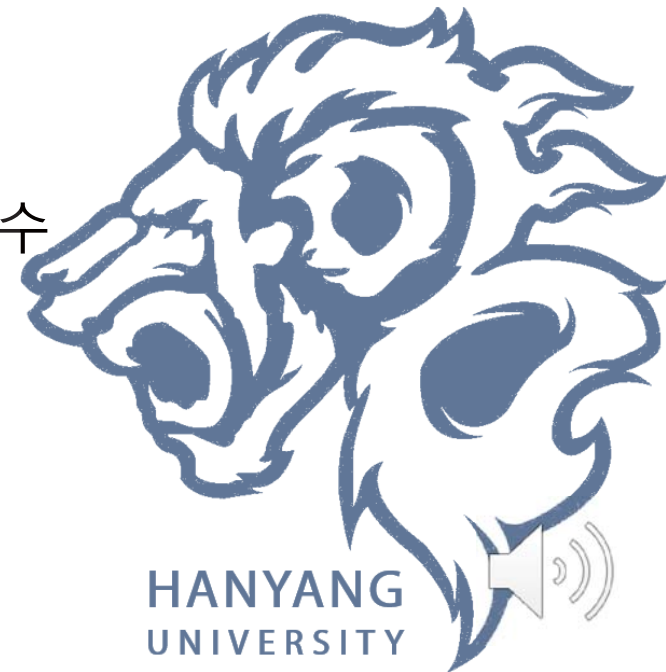
이연준 교수
(한양대학교 ERICA)





Yeonjoon Lee

한양대학교 ERICA 소프트웨어학부 조교수



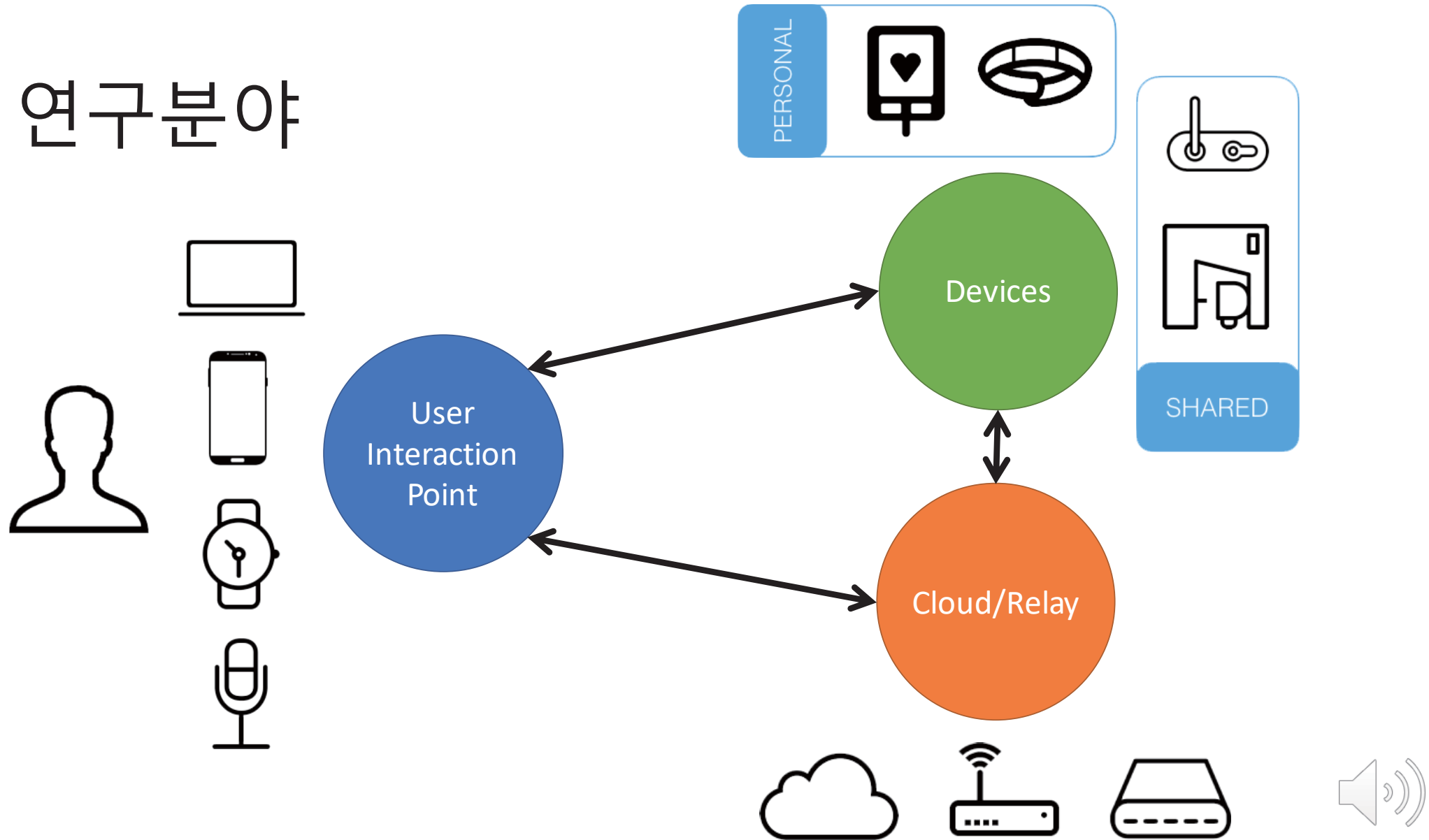
소개



- 소속: 한양대학교 ERICA 소프트웨어학부 조교수
- 박사학위: Indiana University Bloomington (Advisor: XiaoFeng Wang)
- 전공: Security Informatics (정보보안)



연구분야



Publication List

- **Yeonjoon Lee**, Yue Zhao, Jiutian Zeng, Kwangwuk Lee, Nan Zhang, Yuan Tian, Kai Chen, XiaoFeng Wang, Faysal Hossain Shezan. SPEAKER-SONAR: A Sonar-based Liveness Detection System for Protecting Smart Speakers Against Remote Attackers. [UbiComp](#), 2020.
- **Yeonjoon Lee**, Xueqiang Wang, Kwangwuk Lee, Xiaojing Liao, XiaoFeng Wang. Understanding Illicit UI in iOS apps Through Hidden UI Analysis. [TDSC](#), 2019.
- **Yeonjoon Lee**, Xueqiang Wang, Kwangwuk Lee, Xiaojing Liao, XiaoFeng Wang, Tongxin Li, Xianghang Mi. Understanding iOS-based Crowdturfing Through Hidden UI Analysis. Accepted at USENIX [Security](#), 2019.
- Yi Chen, Wei You, **Yeonjoon Lee**, Kai Chen, XiaoFeng Wang, Wei Zou. Mass Discovery of Android Traffic Imprints through Instantiated Partial Execution. In [CCS](#), 2017.
- Soteris Demetriou, Nan Zhang, **Yeonjoon Lee**, XiaoFeng Wang, Carl A Gunter, Xiaoyong Zhou, Michael Grace. HanGuard: SDN-driven protection of smart home WiFi devices from malicious mobile apps. In [WISEC](#), 2017.
- **Yeonjoon Lee**, Tongxin Li, Nan Zhang, Soteris Demetriou, Mingming Zha, XiaoFeng Wang, Kai Chen, Xiaoyong Zhou, et al., Ghost Installer in the Shadow: Security Analysis of App Installation on Android. In [DSN](#), 2017.
- Kai Chen, Xueqiang Wang, Yi Chen, Peng Wang, **Yeonjoon Lee**, XiaoFeng Wang, et al., “Following Devil's Footprints: Cross-Platform Analysis of Potentially Harmful Libraries on Android and iOS”. In [S&P](#), 2016.
- Kai Chen, Peng Wang, **Yeonjoon Lee**, XiaoFeng Wang, Nan Zhang, et al., “Finding Unknown Malice in 10 Seconds: Mass Vetting for New Threats at the Google-Play Scale”. In USENIX [Security](#), 2015.
- Soteris Demetriou, Xiaoyong Zhou, Muhammad Naveed, **Yeonjoon Lee**, et al., “What’s in Your Dongle and Bank Account? Mandatory and Discretionary Protection of Android External Resources”. In [NDSS](#), 2015.
- Tongxin Li, Xiaoyong Zhou, Luyi Xing, **Yeonjoon Lee**, Xiaofeng Wang, Xinhui Han, “Mayhem in the Push Clouds: Understanding and Mitigating Security Hazards in Mobile Push-Messaging Services”. In [CCS](#), 2014.
- Xiaoyong Zhou, **Yeonjoon Lee**, Nan Zhang, et al., “The Peril of Fragmentation: Security Hazards in Android Device Driver Customizations”. In [S&P](#), 2014.



Research Area

- **Mobile Systems Security**

- Vulnerabilities in Android app installation
- Vulnerabilities in Android device driver customization
- Vulnerabilities in Mobile push-messaging service

- **Mobile Malware Detection and Identification**

- Detection of hidden-UI based malware
- Detection of repackaged malware
- Detection of iOS malware based on cross-comparing with Android
- Identification of malware based on network signatures

- **IoT Security**

- Router-based protection for IoT devices
- Sonar-based protection for voice interfaces of smart speakers



Understanding iOS-based Crowdturfing Through Hidden UI Analysis

USENIX Security 2019



Introduction

- **Fake reviews**
 - yelp reviews, amazon reviews
- **Fake news**
 - Spreading rumors through posts or twitter
- **Fake accounts**
 - Fake accounts on online stores
- **Fake app reviews or installation**
 - App ranking manipulation

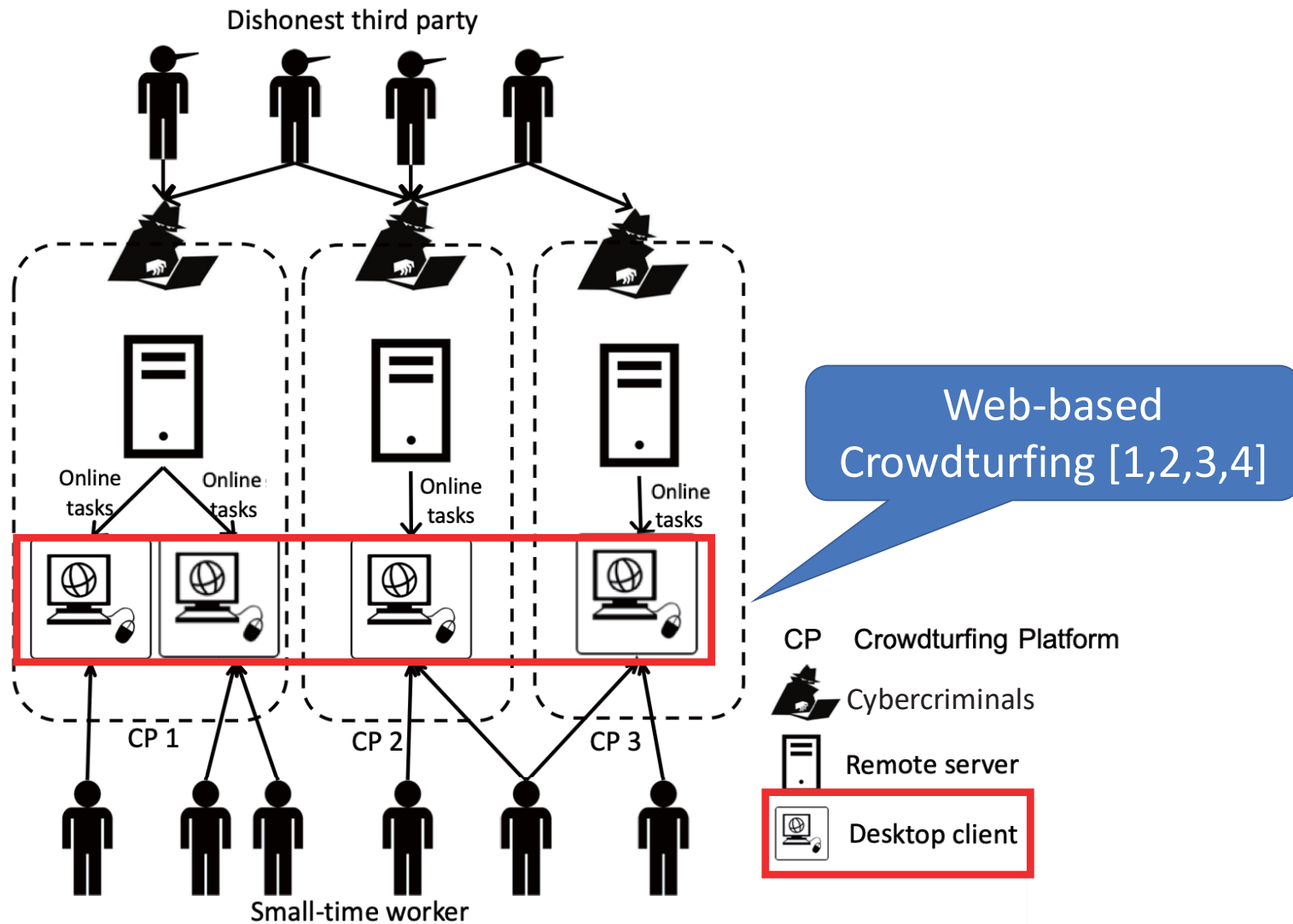


Crowdturfing: definition

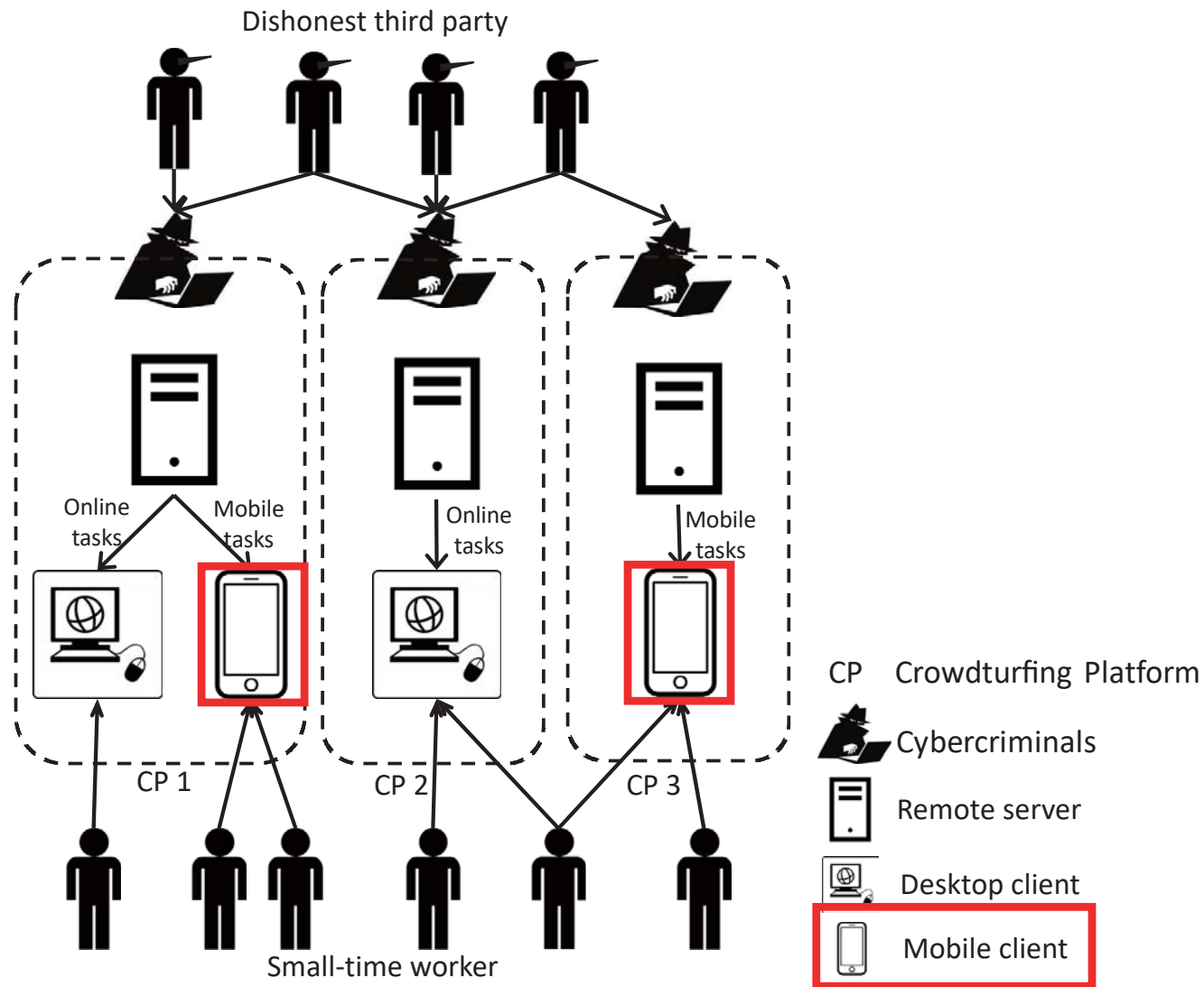
- **Crowdturfing:** malicious crowdsourcing
 - It is an illicit business model, in which *Cybercriminals* recruit *small-time workers* to carry out *malicious tasks* for *dishonest third parties*.



Crowdturfing: platform

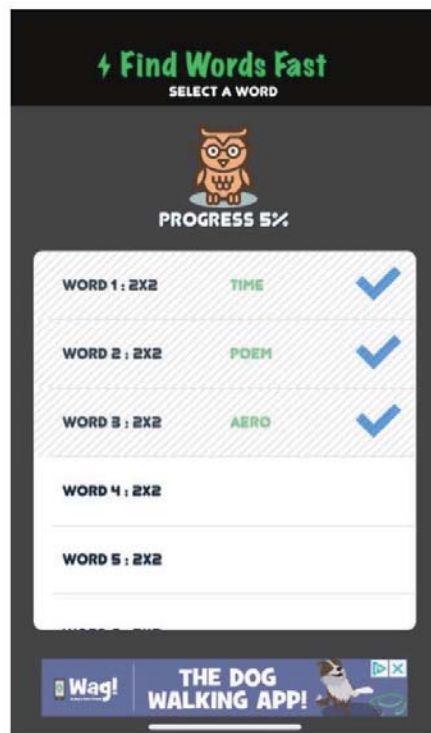


Crowdturfing: platform

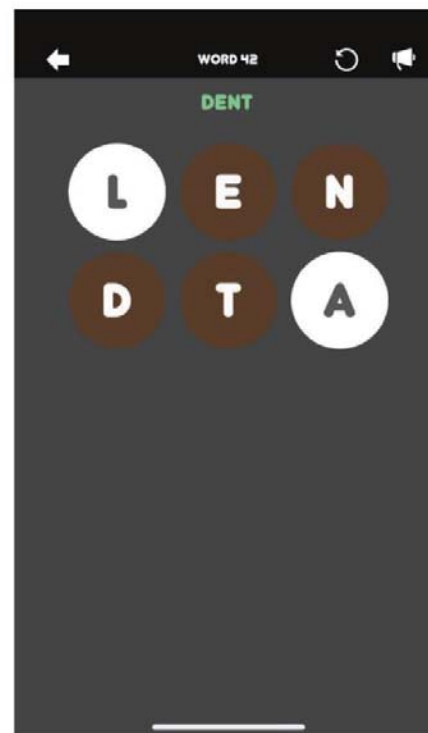


Crowdturfing apps

Word Game UI

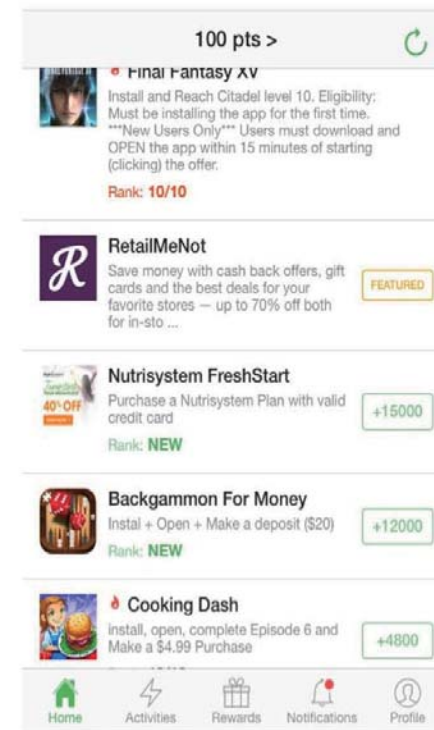


Game list



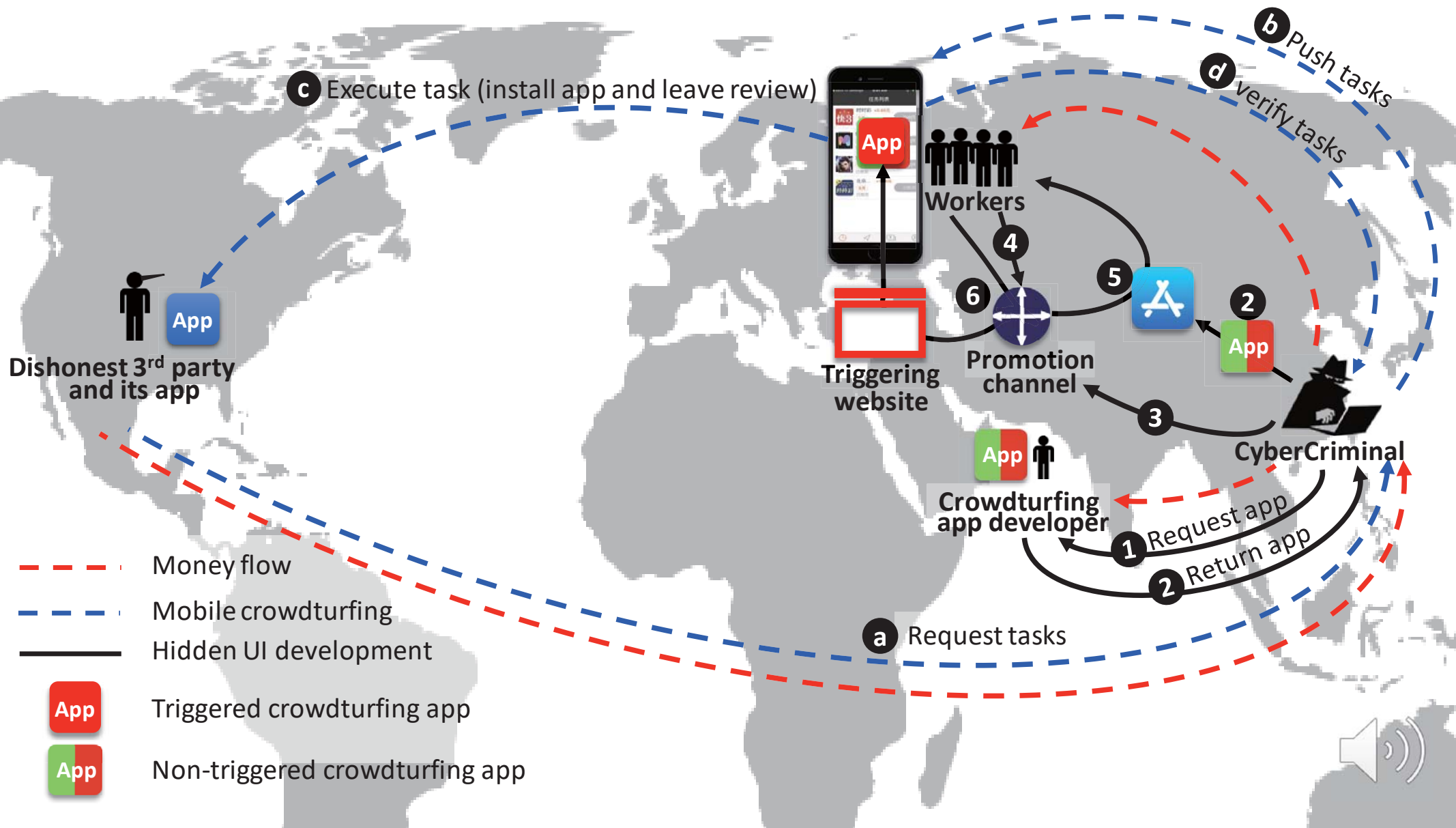
Game UI

Crowdturfing UI



Task list





Q&A

- Email: yeonjoonlee@hanyang.ac.kr
- Website: yeonjoonlee.com



제53회
2020 온라인 춘계학술발표대회

신진학자 워크숍

하드웨어 기능을 활용한 임베디드 시스템 보안 연구

권동현 교수
(부산대학교)



하드웨어 기능을 활용한 임베디드 시스템 보안 연구

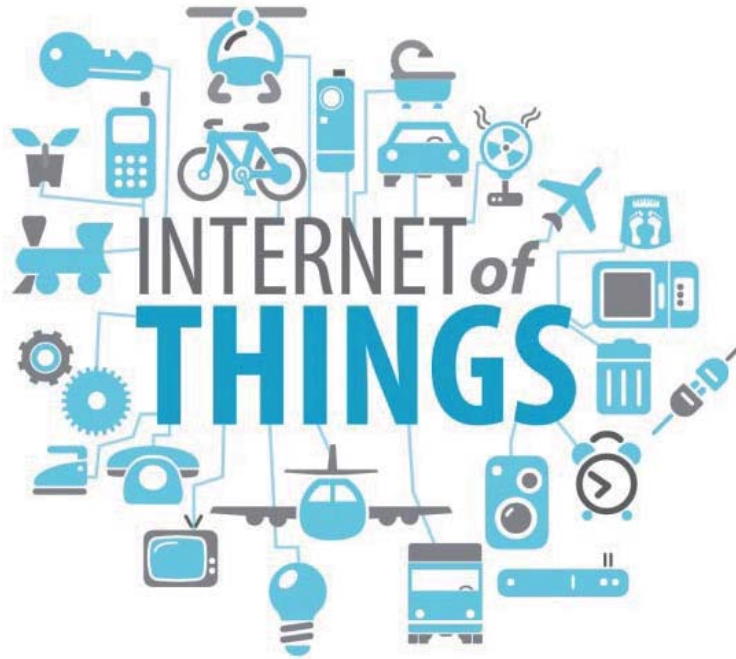
부산대학교 정보컴퓨터공학부
권동현 교수



부산대학교
PUSAN NATIONAL UNIVERSITY

Embedded System Security

- 사물인터넷 시대 도래
- 임베디드 시스템의 보안 중요성 증대
 - 스마트 TV 등 스마트 가전에 탑재된 카메라 해킹
 - 임베디드 기기가 탑재된 의료기기의 오동작 유도
 - 스마트 카에 탑재된 센서 정보 변조



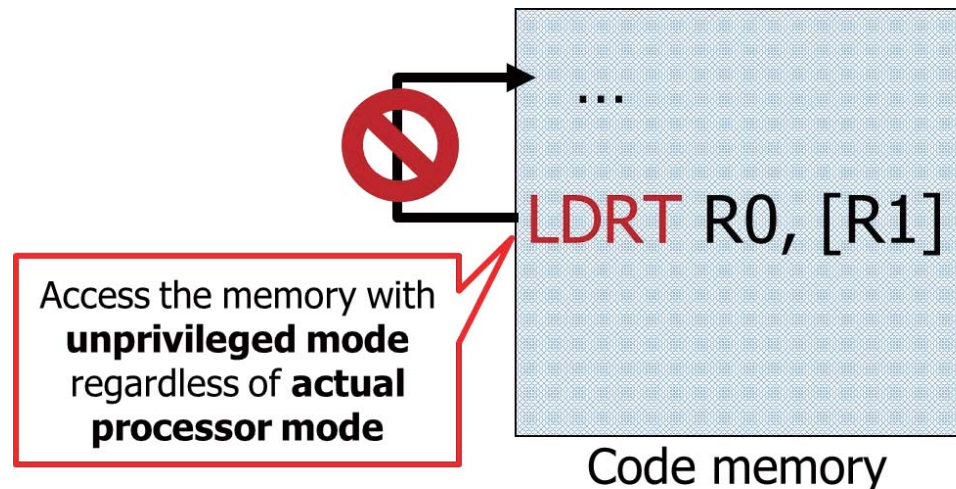
But, in low-end embedded systems..

- Constrained computing resources
 - Low cost, low power consumption
 - Small memory, Low CPU clock speeds
- Lack of processor architectural supports
 - No MMU (no virtualization)
 - Few security extensions



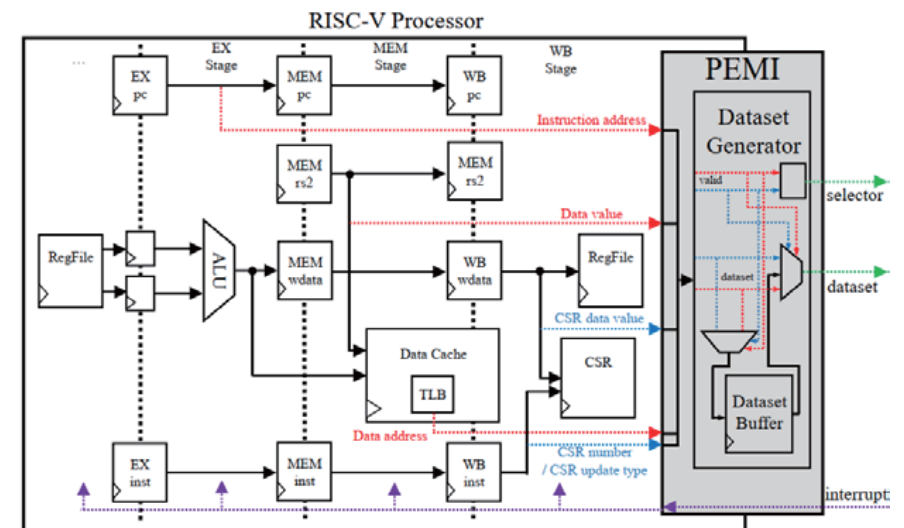
1. Use Existing Hardware Features

- uXOM: Efficient eXecute-Only Memory on ARM Cortex-M
 - Presented at USENIX Security '19
 - eXecute-Only-Memory (XOM)
 - Use as a primitive for many security solutions
 - Already provided in high-end processor architecture
 - uXOM
 - Use unprivileged memory instructions (LDRT, STRT) in ARMv7-M
- Other features
 - ARM TrustZone-M



2. Add New Hardware Features

- RiskiM: Toward Complete Kernel Protection with Hardware Support
 - Presented at Design Automation and Test in Europe (DATE) '19
 - Integrity Monitor
 - Monitor various system behaviors
 - Memory events, system configuration, executed instructions ...
 - Add special hardware interface for this
- Next step
 - Add special instructions for security



Conclusion

- Embedded system security
 - Using existing hardware features
 - Adding new hardware features
- There are opportunities
 - Numerous use cases
 - RISC-V open source ISA
- Contacts
 - E-mail: kwondh at pusan dot ac dot kr
 - Site: <https://sites.google.com/view/csl-pnu>