https://doi.org/10.33778/kcsa.2024.24.2.055

웨어러블 디바이스 보안 위협 및 대응 방안

한 성 화*

요 약

IoT 기술 발전으로 스마트 헬스케어나 스마트 의료서비스도 급격히 발전하고 있다. 이 서비스에 필요한 웨어러블 디바이스는 스마트 밴드 등의 형태로 센서, 컨트롤러로 사용되고 있다. 웨어러블 디바이스는 가능한 장시간 사용을 위해 매우 간결한 SW 로직으로 구현할 뿐만 아니라, 편의성 증진을 위해 무선 통신 프로토콜을 사용한다. 그러나 이 웨어러블 디바이스는 경량성을 추구하고 있어, 다른 정보서비스에 사용되는 단말보다 보안에 취약하다. 본 연구에서는 웨어러블 서비스의 기술적인 운영 환경을 분석, 웨어러블 디바이스에 대한 인증 정보 재사용 공격, BIAS 공격, 배터리 소진 공격, 펌웨어 공격을 식별하고, 각 보안 위협의 메커니즘을 분석하고 공격 효과를 조사하였다. 또 본 연구에서는 식별한 보안 위협에 대한 대응 방안을 제시하였다. 웨어러블 서비스를 개발할 때 본 연구에서 제안한 대응 방안을 고려한다면, 더 안전한 서비스를 구축할 수 있을 것으로 기대된다.

Wearable Device Security Threat Analysis and Response Plan

Sung-Hwa Han*

ABSTRACT

With the development of IoT technology, wearable services have also developed rapidly. Wearable devices required for this service are used as sensors and controllers in the form of smart bands. Wearable devices implement very concise SW logic for possible long-term use and use wireless communication protocols to improve convenience. However, because this wearable device aims to be lightweight, it is more vulnerable to security than terminals used for other information services. Many smart healthcare or smart medical services are passive or do not apply security technology. By exploiting this security environment, attackers can obtain or modify important information through access to wearable devices. In this study, we analyzed the technical operating environment of wearable services and identified authentication information reuse attacks, BIAS attacks, battery drain attacks and firmware attacks on wearable devices. And we analyzed the mechanism of each security threat and confirmed the attack effect. In this study, we presented a response plan to respond to the identified security threats. When developing wearable services, it is expected that safer services can be built if the response plan proposed in this study is considered.

Key words : Wearable Device, Authentication Information Reuse, Security Threat, BIAS, Battery Drain

접수일(2024년 03월 27일), 수정일(1차: 2024년 04월 18일), 게재확정일(2024년 05월 27일)

* 동명대학교/Dept. Information System and Security

1. 서 론

IoT(Internet of Things)는 다양한 사물을 네트워크로 연결하는 개념이다[1]. IoT 기술을 이용하여 다양한 센서와 컨트롤러를 개발할 수 있게 되었으며, 이를 통해 정보기술의 융복합 영역을 확장할 수 있게 되었다. IT 융합 트랜드에 의해, IoT 기술은 스마트 팜이나 스마트 에너지, 스마트 해양으로 확대되었으며, 그 범위는 더 확대되고 있다[2]. 고용량·경량 배터리와 RESTful SW, 고속 무선 통신 기술은, IoT 기반 서비스의 발전 속도와 적용 범위를 급격히 증가시켰다[3]. 이러한 기술 환경에 의해 IoT 기술은, 사람의 건강 유지 및 개선, 질병 치료 등을 위한 스마트 헬스케어나 스마트 의료서비스로 확대되었다[4].

대부분 스마트 헬스케어나 스마트 의료서비스는 개인을 위한 서비스로 중요·민감정보를 취급하며, 사용자 건강 상태를 확인하거나 의료 행위를 지원하기 위해 대부분 웨어러블 디바이스를 사용한다. 웨어러블 디바이스를 사용하여, 사용자에게서 발생하는 다양한 물리·화학적 정보를 수집·전달하거나 진단 결과를 바탕으로 원격 치료를 지원할 수 있다[5].

이러한 웨어러블 디바이스는 사용자의 이동성과 착용 편의성을 위해 경량화된다. 또 충분한 사용 시간 보장을 위해 웨어러블 디바이스에 탑재되는 SW는 경량 SW 아키텍처를 추구한다[6].

스마트 헬스케어 및 스마트 의료서비스도 외부 환경에 의한 간섭이 발생하거나 악의의 공격에 의해 침해받을 수 있다. 특히 경량 SW를 추구하는 웨어러블 디바이스는. 대부분 정보보호 관련 기술 적용에 소극적이거나 배제하기 때문에 보안에 매우 취약하다[7]. 웨어러블 디바이스가 보안 위협에 침해당하면, 잘못된 정보 전달로 사용자 건강 정보가 왜곡될 수 있다. 스마트 의료서비스에서 웨어러블 디바이스가 침해받는다면, 환자의 생명에 심각한 위협이 될 수 있다.

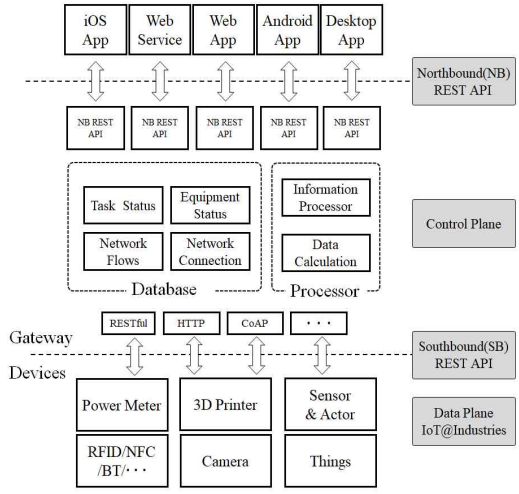
이러한 보안 환경을 개선하기 위해서는 웨어러블 디바이스를 포함한 스마트 헬스케어 및 스마트 의료서비스의 보안 체계를 갖추고, 적절한 보안 기술을 적용해야 한다. 특히 경량성을 추구하는 웨어러블 디바이스의 보안을 강화해야 한다. 이에 따라 본 연구에서는, 스마트 헬스케어나 스마트 의료서비스에 대해 빈번하게 발생하는 보안 위협 중 인증 정보 재사용 공격과 BIAS 공격, 베터리 소진 공격, 펌웨어 공격을 식별·분석하고. 공격 효과를 조사한다. 또, 각 보안 위협에 대응하기 위한 대응 방안을 제시한다.

본 연구에서 식별·분석한 보안 위협 메커니즘과 공격 효과 조사 결과와 대응 방안을 고려하여 스마트 헬스케어나 스마트 의료서비스를 개발한다면, 더 안전한 서비스를 제공할 수 있을 것이다.

2. 관련 연구

2.1 스마트 헬스, 의료서비스 현황

IoT 개념이 확산되면서, 다양한 디바이스가 개발되었다. 고용량 배터리와 무선통신 기술 활용이 확대되면서, 무선 기반 웨어러블 디바이스를 사용하는 스마트 헬스케어와 스마트 의료서비스 개발이 확대되고 있다[8].



(그림 1) IoT 기반 스마트 헬스케어, 스마트 의료서비스 프레임워크

스마트 헬스케어나 스마트 의료서비스의 대표적인 프레임워크는 그림 1과 같다. Data Plane에 속하는 다양한 형태의 디바이스를 통해 데이터를 생성·수집한다. 데이터는 Southbound REST API를 통해 Control

Plane으로 전달된다. Control Plane은 전달받은 정보를 저장하고 처리한다. 사용자는 Northbound REST API를 통해 저장·처리된 정보를 확인한다[9].

스마트 헬스케어나 스마트 의료서비스는 서비스 유지 시간 확보를 위해 SW 아키텍처 경량화를 추구한다. 정보 송수신에 사용되는 컴퓨팅 자원 소모를 최소화하기 위해 많은 서비스가 COAP나 MQTT와 같은 RESTful 구조를 선택하였다[10].

2.2 스마트 헬스케어, 의료서비스의 보안 현황

스마트 헬스케어나 스마트 의료서비스는 착용 편의를 위해 소형 배터리를 사용하며, 무선통신 기술을 적용한다. 이러한 기술 환경에 보안 기술을 적용하면 서비스 오동작이 발생하거나 배터리 급격히 소진되어, 서비스 이용 불편을 야기하며 서비스 이용 시간을 단축시킨다. 이러한 이유로 대부분의 스마트 헬스케어나 스마트 의료서비스는 정보보호 기술 도입에 소극적이거나 보안 기술을 적용하지 않는다[11, 12].

이러한 정보보호 환경에서 악의적 공격자는 보안에 취약한 웨어러블 디바이스를 경유하여 스마트 폰에 접속 후, 원격지 서버에 접속할 수 있다. 이 경우 공격자는, 스마트 폰 사용자의 개인정보는 물론, 스마트 헬스케어나 의료서비스에 필요한 중요 정보를 취득하거나 수정·삭제할 수 있다.

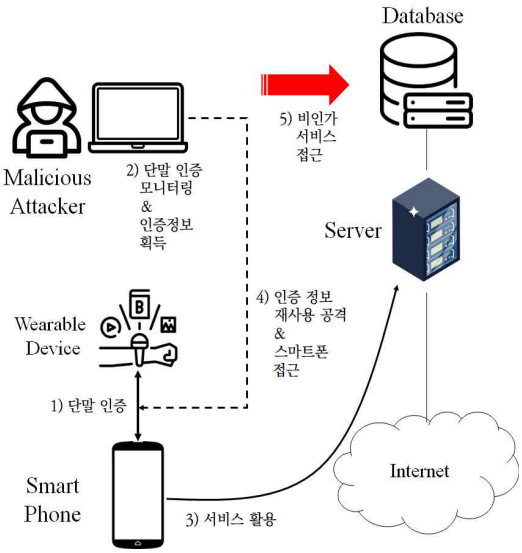
3. 웨어러블 디바이스에 대한 보안 위협

스마트 헬스케어나 스마트 의료서비스는 중요 정보를 취급하며, 침해당했을 때 그 피해 규모가 매우 클 수 있다. 그러므로 이러한 서비스도 악의적 공격으로부터 보호되어야 한다. 본 연구에서는 이러한 서비스에 대한 보안 위협 중, 웨어러블 디바이스를 대상으로 하는 보안 위협 메커니즘을 분석하고 각 공격 효과를 확인한다.

3.1 인증 정보 재사용 공격

웨어러블 디바이스는 일반적으로 사용자의 스마트 폰이나 무선 AP(Access Point)와 연결된다. 웨어러블 디바이스에서 생성된 정보는 스마트 폰을 통해 원격지 서버에 전달된다.

그림 2는 인증 정보 재사용 공격 순서이다. 스마트 폰에서 웨어러블 디바이스를 인증하는 메커니즘은 매우 간단하거나 인증 메커니즘을 적용하지 않는 경우도 많다. 대부분 디바이스 명칭이나 단말 ID가 등록된 정보와 같으면 인증하는 메커니즘을 선택한다. 그러나 이러한 인증 정보는 무선 트래픽 모니터링만으로 충분히 획득할 수 있다. 악의적 공격자는 이를 습득 후 재사용하여 목표한 정보서비스에 접근할 수 있다[13].



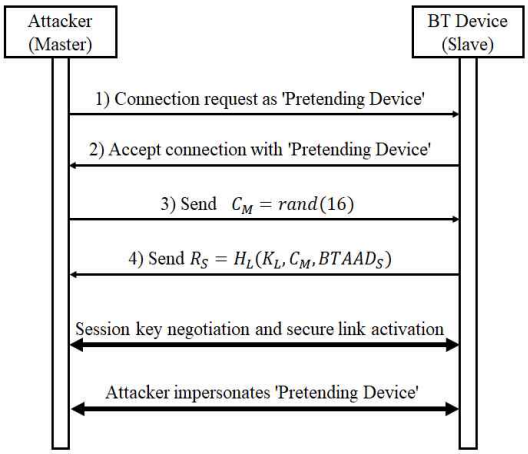
(그림 2) 인증 정보 재사용 공격 메커니즘

3.2 BIAS

BIAS(Bluetooth Impersonation Attacks)는 블루투스 프로토콜에 대한 취약점으로, IEEE Symposium on Security and Privacy에서 발표하였다[14]. 블루투스 통신에서 사용하는 공유 Long-Term Key가 없어도 Slave 단말에 접근할 수 있다. 그림 3은 BIAS 공격 Sequence이다.

두 Bluetooth Device가 처음 연결되면, Long-Term Key를 공유한다. 단말이 서로 다시 연결되어야 할 때는 단말 주소가 같고 공유된 Long-Term Key를 가지고 있다면 상호 인증한다. 그러나 Legacy Connection 방식에서는, Master에서 Slave에 인증되었다는 Message를 전달하면 Slave에서 인증 메커니즘을 적

용하지 않는 취약점이 확인되었다.



(그림 3) BIAS 공격 Sequence

공격자는 위장 대상 단말의 Bluetooth의 주소로 가장하고, Legacy Secure Connection 방식을 사용하여 접속 대상 단말에 Challenge를 보낸다. 이후 Response 값을 받은 후 인증되었다고 응답하면, Long-Term Key가 없어도 대상 단말에 접속(Pairing)할 수 있다. 만약 공격자 단말이 Slave Mode로 동작할 때는, Master 전환(Switch) 요청하면 같은 취약점을 악용할 수 있다. 접속 대상 단말이 Secure Connection 방식을 사용할 때는, 공격자 단말에서 Secure Connection 방식을 지원하지 않는다고 응답하여 Legacy Secure Connection 방식으로 유도하면 이 취약점을 악용할 수 있다.

3.3 베터리 소진 공격

베터리 소진 공격은 웨어러블 디바이스 배터리를 소진하여 단말 및 서비스 가용성을 저해하는 공격으로, 표 1과 같이 크게 네 가지 공격 기법이 있다.

<표 1> 배터리 소진 공격

공격 명	설명
Denial of Sleep	• Random RF Jamming Signal을 목표 단말에게 전송, 통신 불가 상태로 강제 전환시킨다. • 이후 단말은 프레임 수신 및 통신 복구를 위해 Retry를 하며, 이 과정에서 배터리를 소진시킨다.
Flooding attack	• RPL(Routing Protocol for Low Power and Lossy networks) 환경에서 대량의 DIS (DODAG Information Solicitation) message를 공격 대상 단말에 전송한다. • 이후 공격 대상 단말은 DIO (DODAG Information Object) message를 송신하는데, 이 과정에서 목표 단말의 배터리를 소진시킨다.
Vampire -Stretch attack	• 공격 대상 단말에 전송되는 패킷 헤더 정보를 임의로 수정 후 전송한다. • 공격 대상 단말은 인접하지 않은 보다 먼 경로로 트래픽을 전송한다. • 이 경우 배터리를 최대 4배 더 많이 소모한다.
Vampire -Carousel attack	• 공격 대상 단말이 모바일 NW Router일 때 적용하는 방식이다. • 패킷 헤더 수정으로 라우팅 경로를 순환하게 조정한다. • 해당 모바일 NW Router는 트래픽을 순환 처리하면서 배터리를 소진한다.

특히 항상성을 유지해야 하는 스마트 의료서비스가 배터리 소진 공격을 받아 서비스가 중단된다면, 이는 환자의 생명에 심각한 문제를 발생시킬 수 있다[15].

3.4 펌웨어 공격

펌웨어(Firmware) 공격은, 웨어러블 디바이스에 탑재된 펌웨어를 획득하거나 수정, 인가되지 않은 펌웨어를 추가하는 공격이다. 대부분의 스마트 헬스케어나 스마트 의료서비스에서 사용하는 웨어러블 디바이스는 접근통제 기능을 사용하지 않거나 정책 관리에 소홀하다.

이러한 환경에서 공격자는 웨어러블 디바이스에 접근한 후 사용자 권한을 악용, 탑재된 펌웨어를 획득하거나 수정·삭제·임의의 펌웨어를 업로드할 수 있다. 또 Fuzzing 공격 등으로 획득한 펌웨어 업데이트 명령을 사용하여 악성코드가 포함된 펌웨어를 해당 디바이스에 적용할 수 있다[17].

악의적 펌웨어가 업로드되고 실행되면, 웨어러블 디바이스는 오동작하거나 중지될 수 있다. 또 백도어(Backdoor)로 활용되어, 서비스에 접근 후 중요 정보

를 수정·삭제·유출할 수 있다.

4. 웨어러블 디바이스 보안 위협 대응 방안

웨어러블 디바이스를 사용하는 스마트 헬스케어나 스마트 의료서비스에 대한 보안 위협은 갈수록 확대되고 있다. 이러한 보안 환경은 해당 서비스의 활용과 발전을 저해하므로, 이에 대응하여 안전한 서비스를 구축해야 한다. 본 연구에서는 식별된 보안 위협에 대하여 다음과 같은 대응 방법을 제안한다.

4.1 인증 정보 재사용 공격 대응 방안

인증 정보 재사용 공격은 웨어러블 디바이스에 대한 인증 메커니즘을 적용하지 않거나 메커니즘의 보안 강도가 매우 낮을 때 발생할 수 있다.

이를 방지하기 위해서는 단말 등록을 한 후, 초기 접근시나 주기적으로 단말을 검증하는 메커니즘을 적용해야 한다. 단말 ID는 물론, 단말 등록 시 Watermaking 기능을 적용한 식별 및 인증 데이터를 사용해야 한다. 필요하다면 Challenge-Response 방식의 OTP(One Time Password)를 적용할 수 있다.

4.2 BIAS 공격 대응 방안

BIAS 공격은 블루투스 프로토콜 취약점을 악용한 공격 기법이다. 이를 방지하기 위해서는, 블루투스 프로토콜을 사용할 때 Secure Connection을 사용하며, 동시에 하위 버전 호환을 차단해야 한다. 또 단말의 역할(Role, Master/Slave) 전환 차단 메커니즘을 블루투스 프로토콜에 적용해야 한다.

4.3 배터리 소진 공격 대응 방안

배터리 소진 공격은 웨어러블 디바이스에서 활용하는 네트워크 취약점을 이용한 공격으로, 공격 방식마다 그 메커니즘이 다르다. 그러므로 이를 방지하기 위해서는 공격 유형별 다른 대응 메커니즘을 적용해야 한다.

Denial of Sleep 공격에 대응하기 위해서는 Protocol Error 확인 시 Retry 적용을 통한 Sleep 기능을 강제해야 한다. Flooding attack을 방지하기 위해서는 대량의 DIS message 수신에 대한 Anti-DDoS 기능을 탑재해야 한다. Vampire attack은 라우팅 기능의 취약점을 이용한 것이므로, Single/Dual Static Routing Table만을 적용하는 기능을 적용해야 한다.

4.4 펌웨어 공격 대응 방안

펌웨어 공격은 공격자가 웨어러블 디바이스에 탑재된 펌웨어에 접근할 수 있는 취약점을 이용한다.

이 공격을 방지하기 위해서는 서버측의 펌웨어 배포 체계의 보안을 강화하고, 사용자 계정 및 권한 관리를 엄격히 적용하여 웨어러블 디바이스에 탑재된 펌웨어에 대한 접근을 통제해야 한다.

5. 결 론

스마트 헬스케어나 스마트 의료서비스는 현재도 다양한 서비스 형태로 제공되며, 앞으로 더욱 확대될 것으로 예상된다. 특히 원격 진료가 법적으로 가능해지면 그 발전 속도는 더욱 증가할 것이다.

이러한 환경에서 IoT 기반 웨어러블 디바이스를 사용하는 서비스는 아직 보안에 취약하다. 대부분의 서비스가 활용 편의성을 위해 경량화를 선택하여, 서버에 탑재되어 동작하는 SW뿐만 아니라, 웨어러블 디바이스의 SW도 보안 기술 선택에 소극적이다. 이러한 환경에서는 다양한 보안 위협이 발생할 수 있다.

본 연구에서는 웨어러블 디바이스의 보안 취약점을 이용한 인증 정보 재사용 공격과 BIAS 공격, 배터리 소진 공격, 펌웨어 공격을 식별하고, 각각의 메커니즘과 공격 결과를 확인하였다. 이러한 보안 위협이 스마트 헬스케어나 스마트 의료서비스에 가해지면, 악의적 공격자는 인가되지 않은 정보를 취득하거나 임의의 데이터를 주입·변조·삭제를 할 수 있다. 이에 따라 본 연구에서는 이러한 보안 위협에 대한 대응 방안을 제시하였다.

본 연구에서 제안하는 방법을 스마트 헬스케어나 스마트 의료서비스 개발 시 고려한다면, 단말을 통한

정보 유출이나 위변조, 단말의 오동작을 방지할 수 있을 것으로 예상된다.

참고문헌

[1] S. Madakam, R. Ramaswamy & S. Tripathi, "Internet of Things (IoT): A literature review," Journal of Computer and Communications, Vol.3, No.5, pp.164-173, 2015.

[2] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour & E. H. M. Aggoune, "Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk," IEEE access, Vol.7, pp.129551-129583, 2019.

[3] B. Di Martino, A. Esposito, S. A. Maisto & S. Nacchia, "A semantic IoT framework to support RESTful devices' API interoperability," In 2017 IEEE 14th International Conference on Networking, Sensing and Control, IEEE, pp.78-83. May. 2017.

[4] J. Srivastava, S. Routray, S. Ahmad & M. M. Waris, "Internet of Medical Things (IoMT)-based smart healthcare system: Trends and progress," Computational Intelligence and Neuroscience, 2022.

[5] V. Chang, Y. Cao, T. Li, Y. Shi & P. Baudier, "Smart healthcare and ethical issues," In 1st International Conference on Finance, Economics, Management and IT Business, pp.53-59, SciTePress, May. 2019.

[6] J. Shafi & A. Waheed, "Role of smart wearable in healthcare: wearable Internet of Medical Things (WIoMT)," In The IoT and the Next Revolutions Automating the World, pp.133-155, IGI Global, 2019.

[7] P. K. D. Pramanik, P. K. Upadhyaya, S. Pal & T. Pal, "Internet of things, smart sensors, and pervasive systems: Enabling connected and pervasive healthcare," In Healthcare data analytics and management, pp.1-58, Academic Press, 2019.

[8] S. Jeong, J. H. Shen & B. Ahn, "A study on smart healthcare monitoring using IoT based on blockchain," Wireless Communications and Mobile Computing, pp.1-9, 2021.

[9] Z. Wen, X. Liu, Y. Xu & J. Zou, "A RESTful framework for Internet of things based on software defined network in modern manufacturing," The International Journal of Advanced Manufacturing Technology, Vol.84, pp.361-369, 2016.

[10] D. B. Ansari, A. U. Rehman & R. Ali, "Internet of things (iot) protocols: a brief exploration of mqtt and coap," International Journal of Computer Applications, Vol.179, No.27, pp.9-14, 2018.

[11] M. Saleh, N. Z. Jhanjhi, A. Abdullah & R. Saher, "Design Challenges of Securing IoT Devices: A survey," International Journal of Engineering Research and Technology, Vol.13, No.12, pp.5149-5165, 2020.

[12] E. Kim, J. Kim, J. Park, H. Ko & Y. Kyung, "Tinyml-based classification in an ecg monitoring embedded system," Computers, Materials and Continua, Vol.75, No.1, pp.1751-1764, 2023.

[13] H. K. Cho & K. H. Lee, "A Method of Digital Signature Using FIDO2 CTAP," Journal of the Korea Institute of Information Security & Cryptology, Vol.29, No.5, pp.1049-1062, 2019.

[14] D. Antonioli, N. O. Tippenhauer & K. Rasmussen, "Bias: Bluetooth impersonation attacks," In 2020 IEEE symposium on security and privacy (SP), pp.549-562, IEEE, May. 2020.

[15] R. Smith, D. Palin, P. P. Ioulianou, V. G. Vassilakis & S. F. Shahandashti, "Battery draining attacks against edge computing nodes in IoT networks," Cyber-Physical Systems, Vol.6, No.2, pp.96-116, 2020.

[16] M. Eceiza, J. L. Flores & M. Iturbe, "Fuzzing the internet of things: A review on the

techniques and challenges for efficient vulnerability discovery in embedded systems," IEEE Internet of Things Journal, Vol.8, No.13, pp.10390-10411, 2021.

[17] X. Feng, X. Zhu, Q. L. Han, W. Zhou, S. Wen & Y. Xiang, "Detecting vulnerability on IoT device firmware: A survey," IEEE/CAA Journal of Automatica Sinica, Vol.10, No.1, pp.25-41. 2022.

〔저자소개〕

한 성 화 (Sung-Hwa Han)
동명대학교 정보보호학과 교수
숭실대학교 공학박사
관심분야 : IT융합보안, 시스템보안, 인공지능, 악성코드 탐지, 제로트러스트 보안
email: shhan@tu.ac.kr