정 보 보 호 학 회 지
제27권 제1호, 2017. 2

사용자 상황인지 기반 네트워크 보안 구조 연구

이 소 라*, 고 상 준*, 조 금 환*, 김 소 영*, 김 은 수*, 고 훈*

요 약

컨텍스트가 필요한 서비스 및 스마트 기기의 수가 증가함에 따라, 사용자에게 편의성과 유연한 보안성을 탑재한 새로운 보안 정책의 필요성이 강조되고 있다. 특히 현재의 보안 기술을 사용하는데 많은 어려움을 겪고 있는 어린이나 노인, 장애인 등의 IT 취약 계층을 위한 새로운 보안 정책은 절실하다. 편의성과 유연한 보안 정책은 사용자의 서비스 이용 패턴, 위치 등과 같이 공격 상황을 판단할 수 있는 정보를 수집, 분석하여 사용자에게 적합한 보안 서비스 제공 기술이 정의되어야 한다. 본 연구는 언급한 요구사항들을 반영한 사용자 상황인지 기반 네트워크 보안 아키텍처 설계, 사용자 상황인지 데이터 수집, 사용자 상황 분석 플랫폼 연구 그리고 상황인지 기반 보안 어플리케이션 연구 및 분석을 담고 있다.

Ⅰ. 서 론

IoT 기술이 발전하고 상용화가 진행됨에 따라서 다양한 이동형 스마트 기기에 대한 보안 위협이 증가하고 있으며, 최근의 연구 보고서에 세탁기, 냉장고 등에 악성코드가 설치될 수 있는 공격, 자동차가 원격에서 해커에 의하여 불법적으로 제어될 수 있는 공격, 맥박 조정기 등 의료 장치에 대한 보안 취약점이 소개되었다. 이러한 위협에 대응하기 위해, 다양한 보안 솔루션이 제시되었으나, 사용자 편의성 및 경제성에 대한 고려가 없기 때문에 오히려 사용자 불편을 가중시킨다. 예를 들어, 인터넷 뱅킹에서 사용하는 공인인증서는 소프트웨어 토큰의 문제점을 해결하기 위하여 안티-바이러스 소프트웨어, 방화벽, 키보드 암호화 등의 추가 소프트웨어와 OTP와 같은 하드웨어 토큰 사용을 강제화 하여 사용자가 불편함을 느낀다. 향후, 모든 기기의 네트워크 연결이 급속도로 진행됨에 따라서 네트워크 보안 문제는 앞으로 보다 더 중요해질 것으로 판단되며, 특히 현재 보안 솔루션을 이해하고 적용하는 데 어려움을 겪고 있는 어린이나 노인, 장애인 등의 IT 취약 계층을 보호할 필요가 있다.

보안 연구의 흐름은 시스템의 보안성을 유지하면서 사용자 편의성을 높이는 방향으로 연구가 진행되고 있으며, 보안 솔루션의 요구사항으로 얼마나 사용자가 불편함을 느끼는지 여부가 중요하게 언급되고 있다.

근본적인 문제를 해결하기 위해서는 보안 위협에 대한 원리를 정확히 파악하고 현재 솔루션들이 간과하고 있거나 충족하지 못하는 요소들을 보완하는 노력이 필요하다. 사용자 상황인지 기반 네트워크 보안 기술은 일반 사용자에게 편리성과 보안성을 동시에 제공할 수 있는 보안 프레임워크로서, 사용자의 위치정보, 서비스 이용 패턴 등과 같이 상황을 판단할 수 있는 정보를 수집하여 사용자에게 가장 적합한 보안 서비스를 자동으로 제공한다. 따라서 본 연구에서는 사용자 기기의 센서 및 주변 통신기기로부터 데이터를 수집하고 기계학습, 실시간 빅데이터 분석 기술 등을 통해 사용자 주변 상황을 인지하여 최적화된 보안 서비스를 위해 필요한 사용자 상황인지 기반 기술을 설명한다.

Ⅱ. 사용자 상황인지 기반 네트워크 보안기술 동향

2.1. 데이터 수집

[1]논문에서는 보안 측면에서 어떠한 문제점이 있는지 어떻게 이를 해결할 수 있는 지에 대해 소개한다. 디바이스에서 데이터를 수집 할 때, 편리하고 확장성을 보장할 수 있도록 수집하는 여러 방식 중, People-centric Opportunistic Sensing 방식이 활발하게 연구되고 있다. People-centric Opportunistic Sensing이란 사람들이 일상생활에 쓰이는 기기들 (예: Smartphone, Smartwatch

* 성균관대학교

등)을 통해서 센싱을 하고 그 센싱 한 결과들을 WiFi에 연결이 될 때마다 데이터베이스 서버로 보내서 데이터를 수집하는 방식이다. 이런 opportunistic sensing model은 대규모의 데이터를 별도의 기반시설을 배치하지 않고도 수집할 수 있다는 장점이 있지만 데이터 수집하는 참여자의 프라이버시에 관한 문제, 또는 수집된 데이터의 무결성 및 이용 가능성, 등의 문제들이 발생할 수 있다.

[2]논문에서는 디바이스 기기 자체의 보안성과 사용자 프라이버시에 대해 서술하였다. 기기들의 발전에 따라 상황인지 기반 인증 방식에 대해 연구가 활발해지고 있고 상황 인지를 가능하게 하는 데이터들을 수집하는 개인용 스마트 기기들의 시스템 보안성에 대한 연구도 역시 중요하기 때문에, 안드로이드 기기들의 시스템 보안성이 얼마나 악성 앱을 잘 구분하는지를 분석하였다. 안드로이드 기기의 사용이 활발해짐에 따라 다양한 앱들도 안드로이드 마켓에 유통되고 있다. 다만, 마켓에 올라와 있는 대부분의 앱들은 사용자가 앱을 설치 할 때, 기기의 특정 정보들의 접근에 대한 허가(permission access)를 요청하는 경우, 사용자의 개인정보가 유출될 수 있다.

[3]논문은 사물을 사용하는 사용자의 가속도 센서의 패턴이 사물을 구별하는 hallmark가 될 수 있음을 시사했다. 어떠한 주어진 물체에 대해서 실제로 이 물체를 사용하는 사람이 누구인지를 구별하는 것은 중요하다. 사용하는 사용자마다 다른 기능과 인터페이스를 제공할 수 있기 때문이다. 기존 방식은 비밀번호나 지문, RFID 태그 등의 방식을 사용했지만, 이러한 방식들은 추가적인 센서가 필요했다. 따라서 위 논문에서는 손목 모션 센서의 가속도계를 이용했다. 사용자마다 손의 동작이 다르고, 물건마다 다른 인터페이스를 가지고 있다는 점에 착안했으며, 총 가속도 데이터, 중력 데이터, 자이로스코프 데이터를 이용했다. 또한, 사용자가 물체를 사용하는 시점과 손목 모션 센서가 위의 데이터를 수집하는 시점이 일치해야 정확도가 올라간다.

2.2. 컨텍스트 분석

최근의 고도화/대규모화되는 네트워크 인프라를 통한 다양한 보안 위협을 조기에 탐지하여 대처하기 위해서는 체계적인 수단이 필수적이다. 이를 위하여 각종 보안 장비, 네트워크 인프라, 서버/스토리지 장비 및 서비스 응용들로 부터 생성되는 로그, 패킷 등 대량의 이벤트 데이터를 수집하고, 이에 대하여 빅데이터 솔루션을 활용한 보안 분석을 수행하는 보안 관제 체계가 필요하다. 이러한 역할을 담당하는 상용(commercial) 중심의 솔루션이 보안 정보 및 이벤트 관리(Security Information and Event Management: SIEM) 프로그램으로 사용 된다[4-6]. SIEM은 가상/실제 네트워크들, 서비스 응용들, 시스템 로그들과 이벤트 데이터를 수집한 후에 이를 분류하고 분석해서 빠른 보고를 하고, 추가 개입이나 변경된 대응이 필요한 경우는 경고를 수행한다[7]. 또한 본 솔루션이 제공하는 보안 도구들은 기관/기업의 IT 조직에서 보안 관련한 중심 역할을 하는 보안운영센터(security operations center: SOC)의 핵심적인 역할을 담당하고 있다. 솔루션들은 소프트웨어, 장비(appliances) 또는 관리 서비스 형태로 판매하며, 이들은 보안 데이터(security log)를 기록하고 규정 준수(compliance)를 위한 보고서를 생성에도 사용된다[7]. 결국 SIEM의 핵심 기능들은 사용자 및 서비스 권한, 디렉토리 서비스 및 기타 시스템 구성 변경을 모니터링하고 도움을 제공하는 것이며, 추가로 로그 감사/검토 및 사건(incident)별 응답 등을 제공하기도 한다.

Ⅲ. 사용자 상황인지 기반 네트워크 보안 구조 설계

다양한 기기에 대한 보안 위협이 증가함에 따라, 일반 PC에서 사용하던 보안 프로토콜을 그대로 적용하는 것에 대해서 많은 의문점이 생겼다. 따라서 작은 센서 디바이스부터 PC 성능의 안드로이드 디바이스까지 응용 시나리오나 환경에 따라 요구하는 인증 기법이 달라질 수밖에 없다. 본 연구에서는 센서 디바이스가 수집하는 데이터를 이용해, 상황 인지 기반 인증 아키텍처를 설명한다.

3.1. 데이터 수집 아키텍쳐

디바이스에서 수집할 수 있는 데이터의 종류는 매우 다양하다. 스마트폰만 하더라도 10가지 이상의 많은 센서를 부착하고 있고, 하드 센싱 이외에도 소프트 센싱을 통해 사용자의 연락처 정보, 문자 정보 등의 로그도 수집 가능하다. 이러한 데이터들을 각각 fingerprint로 사

용할 수 있다. 예를 들면, 사용자의 평일 GPS 데이터의 패턴은 주로 집과 학교 등 규칙적인 형태를 띌 것이다. 혹은 사용자가 등록되지 않은 전화번호로 걸려오는 통화를 받는 사람은 앞으로도 받을 확률이 높을 것이고, 받지 않는 사람은 앞으로도 받지 않을 확률이 높을 것이다. 이를 바탕으로 사용자가 등록된 사용자가 맞는 지, 혹은 더 나아가 등록된 사용자가 누구인지에 대한 것을 유추할 수 있고 따라서 이는 인증에 사용될 수 있다.

보안 프로토콜에서는 정확도 또한 중요하다. 데이터에서 얻을 수 있는 한 가지를 fingerprint를 attribute라고 하겠다. Attribute 별로 사용자를 구별하는 데에 줄 수 있는 정확도가 다르다. 온도 데이터를 예로 들어보자. 하루 동안에 스마트폰으로 측정하는 온도 데이터의 변화를 보고 사용자를 구분한다고 하면, 이는 상대적으로 오류를 자주 발생시킬 수 있음을 의미한다. 또한 스마트폰의 위치, 사용자의 행동, 현재 날씨, 온/습도 등 다양한 외부 요인이 잡음(noise)을 발생시킬 것이고 이는 사용자를 구별하는 데에 정확도를 낮출 것이다. 다른 attribute도, 기존 패스워드나 인증서 기반의 지식 기반 인증방식에 비해 정확도는 떨어질 수밖에 없다. 따라서 attribute를 이용해 사용자를 구분하기 위해서는, 여러 attribute를 조합하여 신뢰도를 높여야 한다. 일정수준 이상의 신뢰도를 보장하기 위해서는 몇 가지의 attribute 조합이 가능하다.

3.2. 상황인지 기반 다중인자 인증 아키텍쳐

다중 인자 인증(multi-factor authentication)은 자원에 대한 접근 제어를 위하여 인증 대상 사용자에 대해 서로 다른 종류의 정보를 요구한다[5]. 요구받는 정보는 지식 (사용자가 알고 있는)과 소유물 (사용자가 가지고 있는) 등 서로 겹치지 않는 것으로 한다. 일상생활에서는 이미 이러한 인증 방식이 널리 사용되고 있는데, 은행의 현금카드를 통한 거래는 이용자의 확인을 위하여 비밀번호와 현금카드를 함께 요구한다. 이는 각각 지식(비밀번호)과 소유물(현금카드)을 요구하는 것으로 2개의 정보를 요구하므로 다중 인자 인증의 일종인 이중 인자 인증(two-factor authentication)에 해당한다. 이러한 이중 인자 인증은 컴퓨터 시스템과 네트워크에서도 이용이 증가하고 있는데, 구글은 비밀번호와 함께 확인코드 또는 OTP(일회용 비밀번호)를, 애플(Apple)은 비밀번호와 확인코드를 사용하고 있다[8, 9]. 이때 확인코드는 신뢰할 수 있는 기기/전화번호로 요청 즉시 전송된다. 다중 인자 인증이 주로 이중 인자 인증으로 활용되는 큰 이유는 인증 단계가 확장될수록 사용자가 느끼는 불편이 커지기 때문이다. 인증 단계를 줄이기 위하여 구글, 애플은 신뢰하는 브라우저, 또는 신뢰하는 기기에 대하여는 첫 1회에만 이중 인자 인증을 하도록 하여 우회할 수 있는 방법을 제공하고 있다. 그렇지만 이와 같은 방법은 고정된 제한 요건을 두어 편리성을 확보하는 것으로서, 공격자가 신뢰하는 기기에 대한 제어를 확보하거나 사용자가 부주의하게 신뢰하는 기기를 추가하면 무력화될 수 있다.

사용자 상황을 다중 인자 인증의 인증 정보 중 하나로 활용하면 보안 수준을 유지하면서도 편리성을 확보할 수 있다. ‘소프트 센싱’을 통하여 확보한 사용자 상황 정보를 활용하여, 인증 받고자 하는 기기 또는 환경이 사용자가 처한 상황과 부합하는지 여부를 확인할 수 있으므로, 이에 부합하는 경우에만 인증 단계의 복잡성을 완화하여 주는 방식이다. 이러한 방식을 활용하면 사용자 상황 정보와 부합하지 않을 때에는 이중, 삼중의 추가적인 인증 단계를 요구하게 됨으로써 보다 높은 수준의 인증 보안을 달성할 수 있으며, 사용자 상황 정보와 부합하는 경우에는 인증 단계를 간소화하여 사용자 편의를 높일 수 있다. 사용자 상황을 고려한 다중 인자 인증은 다음과 같은 과정으로 인증을 수행할 수 있다.

1) 새로운 기기, 또는 새로운 애플리케이션(앱)에서 로그인을 위하여 인증을 요청
2) 사용자의 ID와 비밀번호를 통하여 첫 번째 단계의 인증을 수행
3) 2)를 통과하면 ‘사용자 상황인지를 통해 사용자가 현재 가지고 있는 것으로 추정되는’ 기기와 인증을 시도한 기기가 같은지, 혹은 같은 상황 정보(물리적 위치, 네트워크 정보 등)를 공유하고 있는지 확인

Ⅳ. 사용자 상황인지 데이터 수집

4.1. 데이터 수집

IoT 시대에 센서 종류들도 많아지고 활용되는 곳도 많아지고 있으며, 사용자가 가지고 있는 기기나 연결된

〔표 1〕 수집 가능한 데이터

Device	Sensors (Physical/ Logical)	Features
Smart phone, PC and ablets/ Wearables	- 폰 정보/콜 - 위치 - 가속도계 - 자기계	사용자의 현재 위치와 활동들
Smart Sensors/ Hub	모션 (Motion) 라이트 (Light)	사용자의 환경과 활동을
Smart Door Lock	위치	집에 있는 사용자 혹은 외부에 있는 사용자
Smart TV with IoT Hub	사용시간 사용자 채널 속성 등	시청시간, 사용자 관심 채널

센서 등으로 사용자의 활동, 행동, 등의 특징들을 뽑아내서 Risk Score를 계산하고 Risk에 따라 적절한 인증 방식을 요청하게 만드는 편리하고 효과적인 인증 방식이다. 수집 디바이스의 종류, Smart Phone, PC, Table PC, Wearable devices, Smart Sensors / Hub, Smart Door Lock, Smart TV with IoT hub, 그리고 다른 연결된 기기들이다. 수집 가능한 데이터는 [표 1] 와 같이 분류할 수 있다[2]. 예를 들어 사용자가 들고 다니는 smartphone이나 wearable devices들의 가속도계(accelerometer), 자기계(magnetometer), 자이로스코프(gyroscope)등의 물리적 센서(하드 센싱)들을 통해 사용자의 위치, 특정 활동(activity) 및 특징(characteristics)를 감지할 수 있으며, 기기의 스크린 상태 (screen state), 배터리 소모량, 전화 기록, 데이터 사용량 등을 감지하는 논리 센서(소프트 센싱)들을 통해 사용자 상황에 적절한 효과적인 인증방식을 요청하게 할 수 있다.

4.2. 보안/프라이버시 이슈

Context-aware opportunistic user authentication System는 사용자의 스마트 기기를 통해 생체 정보 상황들을 수집하고 현재 사용자의 상황을 파악할 수 있음으로 적절한 보안 솔루션을 제공해주는 매력적인 장점이 있다. 반면 이런 데이터 수집으로 인한 사용자 프라이버시에 관한 문제, 수집된 데이터의 무결성 및 이용 가능성, 등의 문제들이 발생할 수 있다. 또는, 스마트 기기들의 사용이 활발해지면서 앱 시장에 악성 앱이 있을 수 있고, 악성 앱이 아니더라도 보안을 고려하지 않는 경우에는 개발자의 실수 등으로 인해 사용자가 광고 등을 통해 실수로 다른 악성 프로그램을 깔려서 개인정보가 유출되는 문제가 발생할 수도 있다[10]. 특히 context aware opportunistic user authentication을 쓰고 있는 사용자라면 해당 기기가 프라이버시 취약 포인트(프라이버시 hole)가 되어가 다른 연결 되어 있는 기기들에 저장 되어 있는 개인정보까지 유출될 위협이 있음을 알게 된다[11].

4.3. 데이터 수집기술

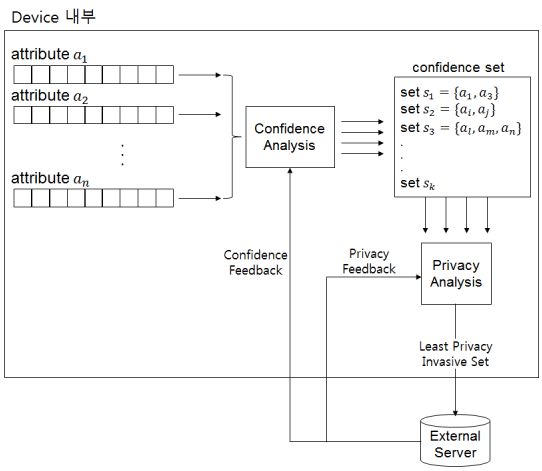
사용자 상황인지를 위한 데이터 수집은 사용자가 운용하는 기기로부터 직접 얻을 수 있는 물리 센서(physical sensor) 정보, 사용자의 습관 및 기기 이용 패턴에 따라 변화하는 논리 센서(logical sensor) 정보, 그리고 여러 가지 센서 정보를 활용하여 새로운 정보를 도출하는 소프트 센싱(soft sensing) 정보 등으로 나눌 수 있다[12, 13]. 각각의 센서 정보들은 GPS 정보와 같이 연속적으로 수집될 수도 있고, 전화 통화 내역과 같이 간헐적으로 수집될 수도 있다. 결국, 상황인지를 위한 데이터는 종류가 다양하고 수집 방법도 일원화하기 어려운 특성이 있다. 따라서 상황인지 데이터는 그것을 이용한 추론을 진행하기 전에 분석 및 가공이 요구된다. 이러한 분석은 처리를 누가 담당하느냐에 따라 구분 가능한데, 사용자 기기에서 센싱한 정보를 바로 처리하는 방법, 그리고 사용자 기기가 데이터를 서버로 전송하여 처리하는 방법이 있다. 사용자 기기에서 직접 처리하는 경우에는 처리 후 데이터 크기가 감소하므로 보관에 용이하고, 서버로 전송하기에도 용이하다. 그러나 사용자 기기가 충분한 성능을 확보하고 있지 못하거나, 데이터 처리에 필요한 알고리즘이 쉽게 업데이트되기 어렵다는 단점이 있다. 한편, 데이터를 서버로 전송하여 처리하는 경우에는 수집된 데이터를 처리함에 있어 충분한 성능을 확보가능하고, 데이터 특성 또는 분석 기준을 변경하여 알고리즘을 업데이트하기에 용이한 장점이 있다. 그러나 수집된 데이터를 모두 서버로 전송해야 하므로 경우에 따라 사용자 기기나 서버에 부담으로 작용할 가능성이 있다.

4.4. 수집 아키텍처

(그림 1)은 제안하는 데이터 수집 아키텍처를 나타낸 것이다. 앞의 절에서 조사한 여러 디바이스에서는 각 디바이스 별로 수집 가능한 데이터가 다양하다. 다양한 데이터 중 각각을 attribute라고 표현하였다. 각 attribute 별로 데이터를 수집하여, 이를 confidence analysis한다. Confidence analysis은 각 attribute 별로 사용자의 fingerprint를 찾는 과정에서 어느 정도의 정확도를 제공하는 지를 분석한다. attribute 1개에 대해서 분석할 수도 있고, 여러 attribute의 조합에 대한 정확도를 분석할 수도 있다. 앞의 관련 연구 파트에서 시사했듯이, attribute의 수가 증가한다고 높은 정확도를 보이지는 않았다. 정확도를 분석하는 것은 처음에는 참고 데이터(reference data)를 기반으로 분석한 후, 머신 러닝을 이용해서 정확도 분석을 계속 학습시킨다. 처음에는 일정 수준 이상의 정확도를 보이지만, 센서 자체의 결함이나 사용자의 패턴 변화 등으로 인해 attribute 별 정확도가 달라질 수 있다. 따라서 후에 인증 결과를 바탕으로, 해당 정확도에 점수(score)를 결정하는 방식으로 업데이트 한다.

Confidence analysis가 끝나면, 일정 임계값 이상의 정확도를 보이는 attribute의 조합이 출력으로 나오게 된다. 임계값은 실험적으로 선택 가능하며, 이 값도 후에 인증 결과를 바탕으로 업데이트 할 수도 있다. 임계값 이상의 attribute의 조합을 confidence set이라고 한다. (그림 1)의 오른쪽에 보이는 것처럼, 총 k개의 confidence set에 대하여 프라이버시 analysis를 수행한다. 프라이버시 analysis는 confidence set에 속한 attribute가 주는 프라이버시에 대해 나타낸다. Attribute 별로 프라이버시에 대한 사용자의 민감도가 다르게 나타날 수 있다. 프라이버시의 민감도를 분석하는 것은 사용자별로 다르기 때문에, 사용자별로 다른 민감도를 적용해야 한다. 민감도를 수치적으로 나타내는 것은 다양한 방법이 있을 수 있다.

예를 들면 사용자가 사용하는 다른 어플리케이션의 접근 권한을 바탕으로 실제로 외부 서버에 데이터를 제공하는 경우에는 민감도를 낮게 설정할 수 있다. 혹은 사용자를 구분하는 것이 더 정확한 경우 민감도를 높게 설정할 수 있다. 예를 들면, GPS 데이터가 가속도 센서보다 더 높은 정확도를 제공한다. 높은 정확도를 제공한다는 것은 사용자를 더 구분하기 쉽다는 뜻이고, 이는 결국 사용자의 개인 정보를 더 정확하게 나타낸다는 의미가 된다. 프라이버시에 대한 분석이 끝난 후, 가장 민감도가 낮은, 즉 사용자의 프라이버시 유출이 가장 덜 한 하나의 집합(set)으로 선정된다. 이렇게 선정된 집합을 least privacy invasive set이라고 하며, Least privacy invasive set을 바탕으로 외부 서버에게 전송한다.



〔그림 1〕 데이터 수집 아키텍처 개요

Ⅴ. 응용: 상황인지 기반 인증 기술

본 섹션은 사용자 상황인지 기반 네트워크 보안 구조를 기반으로 한 응용, 상황인지 기반 인증 기술, 을 설명한다.

5.1. 목적

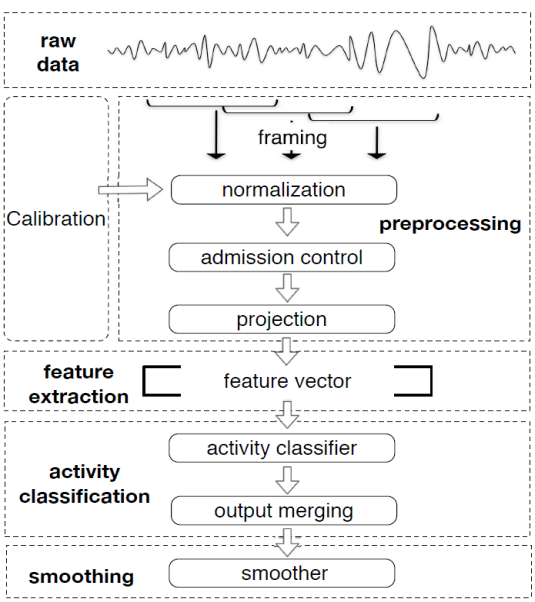
인증이란 허가된 사용자가 실제 그 사용자인지를 판단하는 과정으로 개별 또는 인터넷을 포함한 공공 네트워크에서는 로그인 시 패스워드를 사용해 인증을 한다. 패스워드를 알고 있는 사람은 믿을 수 있는 사용자라고 간주되기 때문에 모든 사용자는 처음에 자신이 원하는 암호를 등록하고, 이후 사용할 때마다 이전에 기록된 패스워드를 잊지 않고 사용해야만 한다. 따라서 많은 사용자들이 기억하기 쉬운 패스워들 사용하거나 하나의 패스워드를 다른 웹사이트에서 사용하는 등의 문제점이 지적되고 있다. 따라서 사용자 상황인지 기반의 인증 기술이 요구된다. 상황인지 기반 서비스를 사용자에게 제

공하기 위해서는 현재 서비스를 사용하고 있는 사용자가 사전에 등록된 적합한 사용자인지 인증하는 절차가 필수적이다.

5.2. 기존 인증 기술의 한계

현재 각종 웹 사이트, 금융거래 등에서 가장 흔하게 사용되는 암호체계는 바로 비밀번호다. 일반 사용자들은 보통 비밀번호를 주로 자신이 기억하기 쉽게 만들어 사용하고 있다. 비밀번호는 쉽게 설정하고 변경할 수 있는 장점이 있지만 비밀번호와 같은 문자 기반의 암호체계는 보통 길이에 따라 보안의 강도가 결정된다.

자신이 기억하기 쉽도록 문자열의 길이가 짧거나 숫자, 영문자, 특수문자 중 한 가지만 사용한 경우, 또한 다른 사람들이 많이 사용하는 일반적인 비밀번호를 사용할 경우에는 공격자들은 비밀번호를 쉽게 풀 수 있게 되고 이로 인해 비밀번호가 유출되거나 사용자의 개인정보까지 유출되게 된다. 그래서 여러 웹 사이트에서는 비밀번호 문자열의 최소 길이를 정해놓거나, 숫자와 영문자 그리고 특수문자의 혼합사용을 필수로 지정하는 등 각자 고유의 비밀번호를 설정하는 기준을 만들어 적용하고 있다. 하지만 사용자들은 하나의 웹 사이트만 사용하는 것이 아니라 여러 웹 사이트와 서비스를 이용하기 때문에 각각의 ID와 비밀번호를 관리하기가 매우 어려워진다. 그래서 사용자들은 주로 동일하거나 유사한 암호를 사용하게 되는데, 만약 그 중 어느 한 곳에서라도 비밀번호가 유출된다면 해당 사용자가 이용하는 다른 웹 사이트나 서비스에서도 정보가 유출되는 등 2차 피해가 발생할 가능성이 높아진다.



〔그림 2〕 가속도 센서 수집 데이터 처리 과정

5.3. 제안 기술

상황인지에 사용하는 정보는 가속도 센서(acceleration sensor), 마이크(microphone), GPS 위치기반서비스, 터치스크린(touch screen)으로부터 수집한다. 가속도 센서는 사용자의 운동 상태와 이동 속도를 측정할 수 있고, 마이크는 사용자의 음성을 입력받을 수 있다. GPS 위치기반서비스는 정확한 사용자의 위치를 파악할 수 있으며, 터치스크린은 사용자의 터치 행동들을 수집할 수 있다[14].

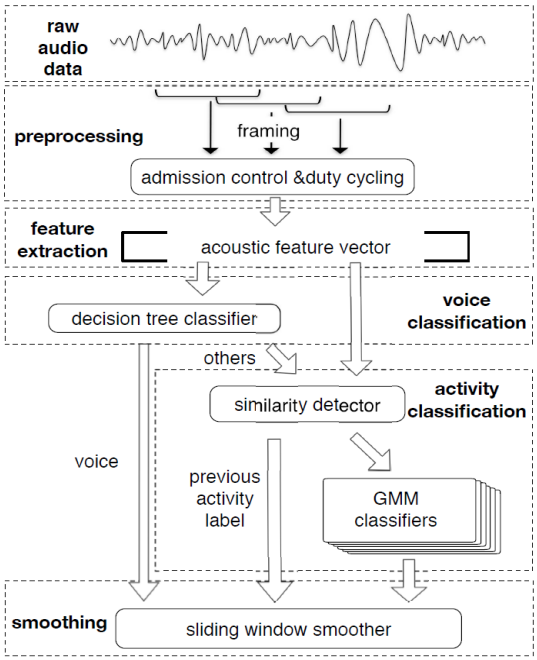
5.3.1. 운동 상태

가속도 센서 내부에는 일종의 지지대가 존재하는데, 중립인 상태에서 가속이 생기게 되면 이 지지대가 휘어지는 정도로 가속도를 측정할 수 있다[15].

가속도 센서를 통해 수집한 데이터는 (그림 2)의 처리 과정을 거쳐 현재 사용자의 운동 상태를 분류한다. 정지 상태, 보행 상태, 사이클링(cycling) 상태, 달리기 상태, 차량 탑승 상태로 구분되며, 각 운동 상태의 사용자 특징과 현재 사용자 특징이 일치하는지 연산하여 사용자를 인증한다.

5.3.2. 음성

마이크는 음성통신 기능에 사용되는 장치이기 때문에 사용자가 통화를 할 때 쉽게 데이터를 확보할 수 있어 자원 소모 문제를 해결할 수 있다. 마이크를 통해 수집한 오디오 데이터는 (그림 3)과 같은 처리 과정을 거쳐 사람의 음성을 추출한 뒤 사용자를 인증한다. 에너지 엔트로피의 표준편차(standard derivation of energy entropy), 영교차율(zero crossing rate), 스펙트럼 롤오프(spectral rolloff), 스펙트럼 무게중심(spectral centroid), 에너지 엔트로피의 평균(the mean of energy



〔그림 3〕 마이크 수집 데이터 처리

entropy), 신호 에너지(signal energy), 스펙트럼 플럭스(spectrum flux) 등 12개의 값을 사용자 인증에 이용할 수 있다.

5.3.3. 사용자 위치 기록

사용자 위치 기록은 사용자의 행동 패턴을 나타내는 정보로서, GPS 위치 기록을 사용자 인증에 이용할 수 있다. 그러나 스마트폰의 자원 소모량을 고려하면 GPS 위치기반서비스를 계속 실행 상태로 유지할 수 없다. 따라서 자원 소모량에 맞추어 GPS 실행 시간 적절한 수준으로 감소시켜야 한다. 위치 기록을 적게 할수록 사용자 인증 정확도가 떨어질 수 있으므로, 사용자의 일반적인 위치 이동 패턴을 학습하여 사용자의 듀티 사이클(duty cycle)에 따른 적응적 샘플링 스케줄링(adaptive sample scheduling)을 적용한다. 가속도 센서의 정보를 이용해 사용자의 운동 상태를 결정하면, 운동 시에만 GPS 센서를 실행 할 수 있다.

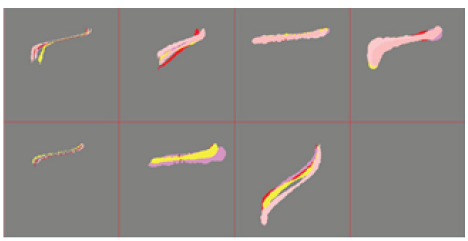
5.3.4. 멀티터치(multi-touch)

스마트폰 터치 제스처(touch gesture)는 밀기(flick), 모으기(pinch), 벌리기(spread) 등 세 가지로 분류할 수 있다(그림 4).

터치 제스처는 스크린을 누르는 시간, 방향, 힘 등에 의해 사용자에 따라 다르게 나타나기 때문에 각 제스처를 3가지의 카테고리(touch 모션의 시작부분, touch 모션의 메인 부분, touch 모션의 마지막 부분)로 구분하였다. (그림 5)는 밀기 제스처(flick gesture)를 설명한다. 터치의 압력에 따른 trace dot의 크기를 통해 해당 trace를 관찰해보면, 각 trace에 대하여 터치의 가속도, 안정적인 속도의 움직임, 터치의 감속도가 있음을 알 수 있다. 각 제스처는 사용자에 따라 다르게 나타남을 보여주며, 이런 제스처의 특징들을 종합하여 사용자 인증을 할 수 있다[16]. 또 한 가지 방법은 키 입력 패턴(keystroke dynamics)을 이용하는 것이다. 키 입력 패턴은 사용자 개개인이 키보드나 스마트폰 터치를 할 때, 자신만의 고유한 키 입력 패턴을 가지고 있다는 기본 가정을 갖으며 키 입력 패턴을 사용자의 고유한 특성으로 저장하고 사용자를 인증한다.

예를 들면, 문자 메시지를 보낼 때, 각각의 키패드 버튼을 하나씩 누르는 과정에서 버튼을 하나 눌렀다가 떼는데 소요되는 시간, 다른 버튼을 누를 때까지 소요되는 시간 등 여러 과정의 시간 정보를 이용하여 fuzzy logic, k-nearest neighbor algorithm, neural network, 통계적 값을 이용하는 분류기 등에 적용하여 키 입력 패턴 인증을 실시하여 사용자를 인증할 수 있다[17].

〔그림 4〕 스마트폰 터치 제스처의 종류



〔그림 5〕 사용자에 따른 밀기 제스처(flick gesture) 특성

5.4. 상황인지 기반 인증을 위한 컨텍스트

상황인지 기반 인증을 위한 컨텍스트는 아래 [표 2]에 정의한다.

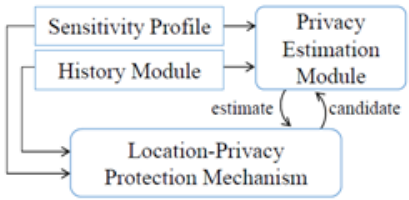
〔표 2〕 상황인지 기반 인증을 위한 컨텍스트

요구 정보		내용	요구 기술
운동 상태		사용자의 운동 상태를 정지 상태, 보행 상태, 사이클링(cycling) 상태, 달리기 상태, 차량 탑승 상태 등으로 분류	가속도 센서, 자이로스코프 센서
음성		주변 소음이 많을 때와 주변 소음이 없을 때를 구분	마이크
위치	실외	사용자가 자주 방문한 실외 장소 파악	GPS
	실내	사용자가 자주 방문한 실내 장소 파악	WiFi AP 접속기록
터치 기록		사용자의 터치 제스처(밀기, 모으기, 벌리기), 전화번호 터치, 문자메시지 보내기, 패턴 인식 등에서 시간이나 압력 특징 추출	터치 패드

5.5. 상황인지 서비스의 고려사항

5.5.1. Privacy-preserving data collection

- **위치 보안**: 상황인지 기반 서비스를 위해서는 사용자들의 상황 정보를 수집해야 한다. 그러나 수집된 상황 정보는 사용자의 프라이버시와 관련 있는 정보일 가능성이 존재하기 때문에 상황인지 서비스를 제공하면서도 사용자의 프라이버스를 보호하는 기술이 요구된다. 예를 들어 사용자의 지리적 위치 정보를 데이터 분석을 위해 서버에 제공한다고 가정하자. 사용자의 위치 정보는 신념, 직업 또는 병원 방문과 같이 알리고 싶지 않은 수많은 정보를 내포하고 있다. 공격자가 노출된 사용자의 위치 정보를 이용해서 더 많은 개인의 정보를 획득할 수 있기 때문에 사용자는 위치 정보 노출을 원하지 않을 것이다. 기존 연구에서는 공격자가 획득한 위치 정보에 혼란을 주기 위해서 위치 정보에 의도적으로 노이즈를 추가하는 기법이 제안되었다[18]. 따라서 아래 (그림 6)과 같은 위치 정보 보호 메커니즘이 요구된다. 사용자에 따라 민감하게 생각하는 장소가 각각 다르기 때문에,



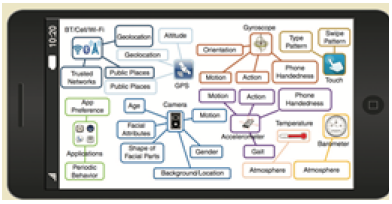
〔그림 6〕 위치 정보 보호 메커니즘

보호 모듈은 사용자의 민감도를 고려한 프로파일을 작성한다. 사용자의 위치가 변경되면, 보호 모듈은 사용자의 프로파일을 확인하여 해당 위치의 노이즈를 결정한다. 즉, 사용자가 민감하게 여기는 장소일수록 큰 노이즈를 추가한다[19].

- **차별적 보안**: 사용자에게 더 좋은 서비스를 제공하기 위해 데이터베이스에 저장된 데이터를 통계적으로 분석하는 방법이 사용된다. 통계적 분석 결과는 모든 사용자 정보가 통합되어 있기 때문에 개개인의 정보를 알 수 없다고 알려져 있지만, 간접적 추론에 의해 유출될 수 있다는 문제가 제기되었다[2]. 예를 들어 통계 데이터로부터 어느 학교의 외국인 교수의 평균 연봉과 외국인 교수의 숫자를 알 수 있을 때, 외국인 교수의 숫자가 한 명이라면 간단한 추론에 의해 해당 교수의 연봉을 알 수 있다. Differential privacy는 어느 한 사람의 정보가 포함된 경우와 그렇지 않은 경우에 대해서 같은 통계적 결과를 만들어 간접적 추론을 방지하는 기술을 말한다. 사용자의 개인 정보를 데이터베이스에 저장할 때, 기존 데이터베이스의 통계적 결과와 수정된 데이터베이스의 통계적 결과를 고려하여 약간의 노이즈를 추가한다. 정보의 정확도를 희생해야 하므로 적절한 균형이 필요한 기술이다.

5.5.2. 신뢰센서

상황인지 기반 서비스를 제공하기 위해 상황 정보를 수집해야 하는데 많은 어플리케이션에서 모바일 기기를 사용한다. 모바일 및 개인 스마트 기기에는 다양한 센서들이 내장되어 있기 때문에 상황 정보 수집에 많이 이용되고 있다(그림 7). 그러나 이러한 센서 데이터는 변조되어 악의적인 목적으로 사용될 가능성이 존재한다. 예를 들어 공격자는 사용자의 스마트 기기에 물리적인 접근이 가능한 사람이고, 해당 기기에 악의적인



〔그림 7〕 모바일 기기에서 사용 가능한 센서 및 기타 액세서리〔20〕

(malicious) 어플리케이션을 미리 설치했다고 가정을 하자. 사용자 기기에서는 센싱을 통해 현재 물리적으로 접근한 사용자에 대한 데이터를 수집하여 스크린 잠금 여부를 결정할 수 있다.

공격자는 사용자의 평소 행동 패턴을 기록한 뒤 설치된 어플리케이션을 통해 센서 데이터를 조작한다면, 현재 물리적으로 접근한 사람이 각 기기 사용자로 오인할 수 있을 것이다. 따라서 수집되는 센서 데이터에 대한 무결성(integrity)이 보장되어야 한다. 따라서 높은 프라이버시 노출이 발생할 가능성이 있는 상황 데이터에 대해서는 수집되는 데이터를 방지하거나 제한함으로써 센서 데이터가 위변조 되는 것을 보호할 수 있을 것이다. 예를 들어 스크린 잠금 해제를 시도하려고 할 때, 다른 어플리케이션에서 해당 데이터에 접근을 하지 못하게 하는 등의 방법이 이용될 수 있다.

5.5.3. 보안 프로토콜

상황인지 기반으로 센싱한 데이터들을 정확하게 분석하기 위해서는 보안의 3요소인 가용성, 무결성, 기밀성 등이 지켜져 시스템이 믿을 수 있는 센싱 데이터를 전달받아 분석할 수 있도록 해야 한다. 만약 네트워크 환경 내에서 데이터 센싱과 분석을 모두 한다면 안전한 데이터 처리를 위한 대표적인 보안 기술인 ARM의 Trustzone [21]를 사용하여 외부로부터 안전한 상황에서 상황인지 처리를 할 수 있다. Trustzone은 최신 ARM 프로세서에 통합 된 하드웨어 보안 기술이다. 프로세서, 메모리 및 주변 장치를 다루는 ARM System-On-Chip(SoC)에 대한 보안 확장으로 구성되어 있다. Trustzone은 OS와 분리 된 보안 서비스를 실행하는데 활용할 수 있다.

Ⅵ. 결 론

사용자 상황인지 기반 네트워크 보안 기술을 실현하기 위해서는 사용자의 위치 정보를 기반으로 한 사용자의 이용 패턴, 이동 패턴 등을 이용한 상황을 판단할 수 있어야 한다. 그리고 안전한 사용자 상황인지 활용을 위해서 사용자 기기의 센서 및 주변 네트워크 기기로부터 데이터를 수집하여, 기계학습, 실시간 빅 데이터 분석 기술 등을 이용해서 사용자 주변 상황을 인지하여 최적화된 보안 서비스를 제시하여야 한다.

본 연구에서는 안전한 사용자 상황인지 서비스 실현을 위해서, 사용자 상황인지 기반 네트워크 보안 기술 동향을 파악했고, 사용자 상황인지 기반 네트워크 보안 아키텍처를 설계하였다. 먼저, 사용자 상황인지 기반 네트워크 보안기술 동향에서는 수집된 데이터의 무결성, 이용 가능성 그리고 사용자 프라이버시 등을 정리한 데이터 수집, 수집된 데이터의 다양한 해석을 위한 분석 단계인 컨텍스트 분석, 그리고 분석된 컨텍스트의 안전한 활용을 위한 컨텍스트 기반 어플리케이션을 정리하였다. 사용자 상황인지 기반 네트워크 보안 아키텍처 설계에서는 클라우드 서버를 기반으로 수집된 상황 정보 분석 및 사용자 주변 상황을 종합적으로 판단하여 위험도를 측정하고, 결과에 따라 사용자의 만족도와 보안성을 충족시킬 수 있는 보안 서비스를 제시하였다. 사용자 상황인지 데이터 수집 단계에서는 상황인지를 위한 데이터를 정의하였고, 디바이스의 종류에 따라 수집할 수 있는 데이터를 구분하고 데이터 종류 별로 데이터를 샘플링 하였으며, 응용단계에서는 상황인지 기반 어플리케이션에서는 상황인지 기반의 어플리케이션, 즉 상황인지 기반 인증 기술 시스템을 제안 및 분석하였다. 마지막으로 상황인지 서비스 고려사항에서는 privacy-preserving data collection, 신뢰센서 그리고 시큐어 프로토콜을 정리하였다.

향후, 본 연구로 마련한 사용자 상황인지 기반 네트워크 보안 아키텍처와 사용자 상황 분석 플랫폼을 바탕으로, 정의한 안전한 상황인지 기반 어플리케이션의 실생활 적용을 위한 후속 연구가 필요하다.

참 고 문 헌

[1] Berker Agir, Jean-Paul Calbimonte and Karl Aberer, “Semantic and Sensitivity Aware Location Privacy Protection for the Internet of Things,” PrivOn'14 Proceedings of the 2nd International Conference on Society, Privacy and the Semantic Web - Policy and Technology, Vol. 1316, pp. 58-63.

[2] Dwork, Cynthia, and Aaron Roth. "The algorithmic foundations of differential privacy." Foundations and Trends in Theoretical Computer Science 9.3-4 (2014): 211-407.

[3] Vishal M. Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges." IEEE Signal Processing Magazine 33.4 (2016): 49-61.

[4] “SIEM: A Market Snapshot,” Dr. Dobb's Journal, Feb. 2007.

[5] J. Hayes, “Cybersecurity and the Big Yellow Elephant,”Cloudera Vision Blog, May 2015.

[6] K. M. Kavanagh, O. Rochford, and T. Bussa,“Magic Quadrant for Security Information and Event Management,”Gartner, Aug. 2016.

[7] Bhatt, P. K. Manadhata, and L. Zomlot, “The operational role of security information and event management systems,” IEEE Security & Privacy, vol. 12, no. 5, 2014.

[8] “Google 2-Step Verification,” Google, retrieved at 2016-11-30.https://www.google.com/landing/2step/

[9] “Two-factor authentication for Apple ID,” Apple, retrieved at 2016-11-30, https://support.apple.com/en-us/HT204915

[10] Gibler, Clint, et al. "AndroidLeaks: automatically detecting potential privacy leaks in android applications on a large scale." International Conference on Trust and Trustworthy Computing. Springer Berlin Heidelberg, 2012.

[11] Kapadia, Apu, David Kotz, and Nikos Triandopoulos. "Opportunistic sensing: Security challenges for the new paradigm." 2009 First International Communication Systems and Networks and Workshops. IEEE, 2009.

[12] H. Witte, C. Rathgeb and C. Busch, "Context-Aware Mobile Biometric Authentication based on Support Vector Machines," 2013 Fourth International Conference on Emerging Security Technologies, Cambridge, 2013, pp. 29-32.

[13] T. Gisby, ““Soft” Sensors Are Breaking Into Four Major Industries,”Aug 2015.

[14] Shi, Weidong, et al. "Senguard: Passive user identification on smartphones using multiple sensors." 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2011.

[15] Juefei-Xu, Felix, et al. "Gait-id on the move: pace independent human identification using cell phone accelerometer dynamics." Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on. IEEE, 2012.

[16] Feng, Tao, et al. "Continuous mobile authentication using touchscreen gestures." Homeland Security (HST), 2012 IEEE Conference on Technologies for. IEEE, 2012.

[17] Araújo, Lívia CF, et al. "User authentication through typing biometrics features." IEEE Transactions on Signal Processing 53.2 (2005): 851-855.

[18] Berker Agir, Jean-Paul Calbimonte and Karl Aberer, “Semantic and Sensitivity Aware Location Privacy Protection for the Internet of Things,” PrivOn'14 Proceedings of the 2nd International Conference on Society, Privacy and the Semantic Web - Policy and Technology, Vol. 1316, pp. 58-63.

[19] Dwork, Cynthia, and Aaron Roth. "The algorithmic foundations of differential privacy." Foundations and Trends in Theoretical

Computer Science 9.3-4 (2014): 211-407.
[20] Vishal M. Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges." IEEE Signal Processing Magazine 33.4 (2016): 49-61.
[21] Santos, Nuno, et al. "Using ARM TrustZone to build a trusted language runtime for mobile applications." ACM SIGARCH Computer Architecture News. Vol. 42. No. 1. ACM, 2014.

〈저 자 소 개〉

이 소 라 (LEE SORA)
학생회원
2015년 8월 : 성균관대학교 컴퓨터공학과 졸업
2015년 9월~현재 : 성균관대학교 소프트웨어플랫폼학과 석사과정
관심분야 : 정보보호

고 상 준 (Ko, Sangjun)
2016년2월 : 한국산업기술대학교, 컴퓨터공학과 졸업
2016년3월~현재 : 성균관대학교, 소프트웨어플랫폼학과, 석사과정
관심분야 : 정보보호

조 금 환 (Geumhwan Cho)
학생회원
2011년 2월 : 청주대학교 정보통신공학과 학사
2013년 2월 : 경희대학교 컴퓨공학과 석사
관심분야 : Usable security, 정보보호, 모바일보안

김 소 영 (Kim, Soyoung)
학생회원
2016년 2월 : 서울여자대학교 정보보호학과 졸업
2016년 3월~현재 : 성균관대학교 소프트웨어대학 석사과정
관심분야 : 정보보호, 네트워크 보안, IoT보안

김 은 수 (Kim, Eunsoo)
2016년 3월~현재 : 성균관대학교, 석사과정
관심분야 : 정보보호, SDN보안

고 훈 (KO, HOON)
1998년 2월 : 호원대학교 컴퓨터학과 졸업
2000년 2월 : 숭실대학교 컴퓨터학과 석사
2004년 8월 : 숭실대학교 컴퓨터학과 박사
관심분야 : 정보보호