DBpia

논문 18-43-05-15 The Journal of Korean Institute of Communications and Information Sciences '18-05 Vol.43 No.05
https://doi.org/10.7840/kics.2018.43.5.878

제스처 센싱을 위한 스마트 퍽 인터페이스의 사용자 보안 인증 모듈 설계

강 시 영◆, 김 정 호°

Module Design of User Security Authentication of Smart Puck Interface for Gesture Sensing

Si-Young Kang◆, Jeong-Ho Kim°

요 약

본 논문은 스마트 퍽 인터페이스를 통한 제스처 인식 모듈의 설계와 다중 사용자를 위한 인증 모듈 설계로 연계하여, 사용자 별 서비스에 대한 보안 개선을 목적으로 한다. 이러한 스마트 퍽 인터페이스를 사용함에 있어, 사용자에게 제공되는 영역의 중복과 그에 따른 충돌(Collision)을 해결하기 위해 LEA(Lightweight Encryption Algorithm)의 재해석과 이에 대응한 사용자 인증 알고리즘으로 MTI(Matsumoto, Takashima, Imai)방법을 선택하여 사용자 인증 모듈을 설계하고 스마트 퍽에 대한 의도적인 공격에 대응한 전송지연과 세그먼트 크기에 따른 정보지연 등 최대 4명의 사용자를 대상으로 한 서비스로 해석하였다.

Key Words : Smart Puck, User Security, LEA, MTI Algorithm, Tangible Interface, Module Design

ABSTRACT

In this paper, It aims to improve the security for each user by linking the design of the gesture recognition module through smart puck interface and the authentication module design for multiple users. In using this smart puck interface, the MTI algorithm is selected as the analysis of the LEA and corresponding user authentication algorithm in order to solve the area overlap an collision which is provided to the user, so we designed the user authentication module and analyzed the four users as service for transmission delays in response to international attack on smart puck and information delay according to segment size.

Ⅰ. 서 론

1.1 연구의 필요성

제4차 산업혁명(the Fourth Industrial Revolution)의 영향으로 기존의 디지털정보화사회는 ICBM(IoT, Cloud System, Big Data, Mobile)[1] 등과 같은 첨단 정보통신 기술이 적용된 초 연결지향(Oriented Hyper Connectivity) 사회로 진화되고 있으며, 제3차 산업혁명에 이어 더 넓은 범위에서 더 빠른 속도로 많은 영향을 미치고 있다. 최근 사물 인터넷이 급부상함에 따라, 기존 산업과 서비스가 융합되고 신기술로서 개발되어 널리 사용되고 있는 추세이며, 이러한 사물 인터넷은 기존의 기술에서 발전되어 더 진보된 기술이 있는가 하면, 기존의 기술에 새로운 기술이 융합되어 또

◆ First Author : (ORCID:0000-0003-4044-1276)Kyungpook National University Department of Electronic Engineering, lamborghini0095@knu.ac.kr, 학생회원
° Corresponding Author : (ORCID:0000-0002-9050-7013)Hanbat National University, Department of Computer Engineering, jhkim@hanbat.ac.kr, 정회원
논문번호 : KICS2018-02-041, Received February 21, 2018; Revised May 2, 2018, 2018; Accepted May 2, 2018

www.dbpia.co.kr

다른 새로운 기술로 탄생되는 형태로 나타나고 있다. 또한, 사물 인터넷과 같은 신기술을 사용하는 사용자는 새로운 기술을 계속해서 선호하고 있고 편리성과 신속성, 간편성이 있는 서비스를 원한다. 이와 맞물려 세계적인 이슈로 정보보안의 문제가 이슈화되고 있으며, 과거 인터넷 접속과 무관했던 디바이스들은 사물 인터넷 환경에서는 인터넷과의 접속으로 기존 인터넷 환경에서 발생할 수 있는 위험 요인이 그대로 발생될 개연성이 커지고 있다.[1]

실제로, 사용자들은 스마트 폰이나 태블릿 PC등 다양한 기기를 통해 새롭고 다양한 정보를 수집하게 된다. 수집된 정보나 데이터는 타 사용자들과 공유하며, 이들 간의 상호 인터페이스에 대한 서비스를 수행 할 수 있지만, 해커들에게 취약점이 노출되어 개인정보를 포함한 각종 정보가 유출되어, 정보보안의 필요성이 증대되고 있다.[1] 한편, 사용자 중심 인터페이스는 기존의 방식에서 지속적인 발전하여 새로운 인터페이스로 거듭나게 되었다.[2,3]

그림 1과 같이 기존의 UI(User Interface)에서 발전된 형태는 GUI(Graphic User Interface)방식이 있고, GUI 방식에서 NUI(Natural User Interface)방식으로, NUI 방식에서 TUI(Tangible User Interface)방식으로 발전하게 되었다. TUI 방식은 디지털 데이터에 대하여 사용자에게 물리적인 조작성을 제공해주는 실감각형 인터페이스 방식으로, 디지털화 된 데이터가 물리적인 객체 등에 적용되어 사용자들의 여가생활에서나 혹은 전시물 형태, 한정된 공간상에서 편리하게 활동할 수 있도록 가능하게 해주는 상호작용 인터페이스 방식이다.

이러한 TUI방식을 채택함으로써 사용자와 시스템 간의 상호작용은 더욱 원활하게 작용하며, 기존의 테이블 탑 디스플레이를 활용하는 NUI방식에 대비하여 단순한 손가락 움직임에 그치는 것이 아닌 사용자들의 편의성과 조작성 등을 극대화시켜 사용자들이 요구하는 시스템과 콘텐츠를 적극적으로 서비스를 수행할 수 있도록 해준다.[2,3]

이렇게 다양한 기술 전개로 사용자들의 요구사항은 더욱 증가되며 극대화되었고 있고, 이를 충족하고자 TUI방식의 콘텐츠들이 등장하여 기존의 테이블 탑 디스플레이에서 새로운 인터페이스인 스마트 퍽 인터페이스(Smart Puck Interface)를 사용하여 다수의 사용자가 동시에 접근을 하지 못하는 문제점이 도출되었다. 이는 3명 내지 4명의 사용자가 동시에 콘텐츠를 이용하고자 할 때 테이블 탑 디스플레이와 그리고 이와 연동되는 스마트 퍽 인터페이스 사이에서 발생되는 사용자에 제공하는 영역 중복과 충돌(Collision)의 문제가 발생한다. 또한 스마트 퍽 인터페이스 하나당 감당하는 영역(Zone)이 사용자간에 겹치면서 오작동을 일으키는 경우를 뜻한다. 즉, 다수의 사용자가 동시에 스마트 퍽 인터페이스를 사용하고자 할 때, 그리고 사용자가 원하는 위치에 맞추어 콘텐츠를 제어하거나 다수의 사용자가 하나의 콘텐츠 내에서 독립적인 형태를 갖는 대상 오브젝트를 제어하고 싶을 때, 제대로 동작이 안 되는 것을 의미한다.[4]

그림 1. 사용자 인터페이스 방식의 변화
Fig. 1. Change the User Interface Type

본 논문은 스마트 퍽 인터페이스를 통한 제스처 인식 모듈의 설계와 다중 사용자를 위한 인증 모듈 설계로 연계하여, 사용자 별 서비스에 대한 보안 개선을 목적으로 한다. 이러한 스마트 퍽 인터페이스를 사용함에 있어, 사용자에게 제공되는 영역의 중복과 그에 따른 충돌을 해결하기 위해 LEA(Lightweight Encryption Algorithm)의 재해석과 이에 대응한 사용자 인증 알고리즘으로 MTI(Matsumoto, Takashima, Imai)방법을 선택하여 사용자 인증 모듈을 설계하고 스마트 퍽에 대한 의도적인 공격에 대응한 전송지연과 세그먼트 크기에 따른 정보지연 등을 4명의 사용자를 대상으로 한 서비스로 해석하였다.[5]

Ⅱ. 본 론

2.1 스마트 퍽 인터페이스

본 논문에서 제스처 센싱을 이용하는 스마트 퍽 인터페이스는 그림 2와 같이 회로도 설계가 되었으며, 그림 3은 설계 회로도에 의한 PCB가 장착된 스마트 퍽 인터페이스 모델이다.[4,5]

스마트 퍽 인터페이스는 Wi-Fi모듈과 MCU가 단일 칩으로 동작하고, 제스처를 위한 센서가 내장되어 있다. 해당 인터페이스를 사용하기 위해서는 그림 4의 테이블 탑 디스플레이는 화면 전체에 전반적으로 터치 센서가 동작되도록 하는 대형 디스플레이 장치이다. 해당 장치를 통해 각종 콘텐츠와 서비스 어플리케이션을 동작하여 사용자들에게 서비스를 제공한다.[6,7]

스마트 퍽 인터페이스를 테이블 탑 디스플레이 상에 놓고 터치스크린과 터치펜을 맞대어 대상 오브젝트를 제어한다. 대상 오브젝트는 사용자가 스마트 퍽

www.dbpia.co.kr

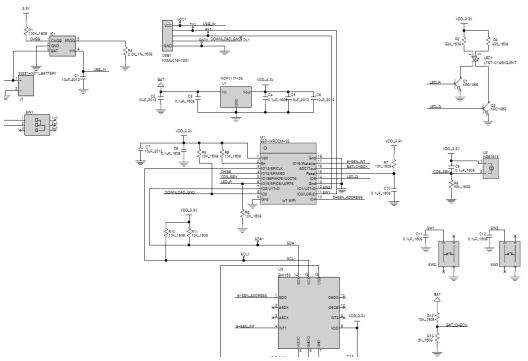

그림 2. 스마트 퍽 인터페이스 회로 설계
Fig. 2. Circuit Design of Smart Puck Interface

그림 3. 스마트 퍽 인터페이스 모델
Fig. 3. Smart Puck Interface Model

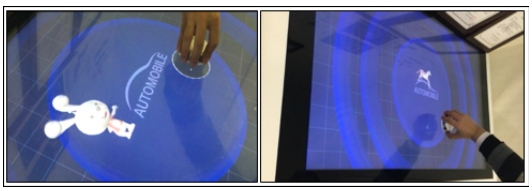

그림 4. 테이블 탑 디스플레이상에서 테스트중인 스마트 퍽 인터페이스
Fig. 4. Testing a Smart Puck Interface on the Table top Display

인터페이스를 움직이는 형태에 따라 좌우로 이동하거나 회전과 드래그 앤 드롭이 가능하도록 되어 있다. 기존에 소형화 장치로서 많이 사용되었던 태블릿 PC의 확장된 형태가 바로 테이블 탑 디스플레이다. 테이블 탑 디스플레이는 현재도 많은 연구와 개발이 이루어지고있으며, 앞으로도 많은 발전이 될 전망이다.

테이블 탑 디스플레이는 멀티 터치도 지원을 하는데, 사용자가 원하면 단일 터치에서 멀티 터치로 전환이 가능하다. 제품에 따라서 성능별 차이가 존재하지만 다수의 사용자가 동시에 멀티 터치를 시도하여도 작동이 되는 만큼 우수한 성능을 보이는 제품도 존재한다. 테이블 탑 디스플레이는 일반적으로 회의용 시스템이나 게임 콘텐츠에 사용이 되며, 전 세계적으로 각광받고 있는 장치로 인식되고 있는 추세이다.[6,7]

2.2 LEA 재해석

LEA는 한국 인터넷 진흥원에서 개발한 ICBM[1]등의 고속(High Speed)환경과 경량(Lightweight)환경에서 기밀성(Confidentiality)을 제공하기 위한 128비트 블록암호 알고리즘이다. Key의 길이는 128bit, 192bit, 256bit로 나뉘며, ARX(Addition, Rotation, XOR) 기반의 GFN(Generalized Feistel Network)구조이다.

성능은 AES에 대비하여 약 1.5~ 2배가량의 빠른 성능을 보이며, S-Box를 배제하여 경량화 구현이 가능하다. LEA는 국내 TTA 표준으로 제정되어 있으며, 이에 따른 규격과 운영모드가 여기에 포함된다. 표 1은 LEA에 대한 규격을 정의한 것이다.[7,8]

표 1에서 N_b 는 평문(Plain Text) 또는 암호문(Cipher Text)을 구성하는 바이트의 개수이며, LEA에 대하여16byte로 고정되어있다. N_k는 비밀 키(Secret Key)를 구성하는 바이트의 개수이며 LEA에 대하여 16, 24 또는 32byte가 사용된다. 마지막 N_r은 라운드의 수를 의미한다. N_k에 따라 결정되며 LEA에 대하여 24, 28, 32byte가 사용된다.[9]

암호화 과정은 K비트 Key K로부터 N_r개의 192bit 암호화용 라운드 Key(1)를 생성하는 Key 스케줄링 함수$KeySchedule_k^{enc}$와 라운드 Key RK_i^{enc}및 라운드 함수 $Round^{enc}$을 이용하여 128bit 평문 P를 128bit 암호문 C로 변환하는 암호화 함수 Encrypt Function으로 구성된다.[9,10]

$$RK_i^{enc}(0 \le i \le (N_r - 1)) \quad (1)$$

복호화의 경우도 마찬가지이다. 192bit 복호화용 라운드 Key(2)를 생성하는 Key 스케줄링 함수 $KeySchedule_k^{dec}$와 Round Key RK_i^{dec}및 라운드 함수 $Round^{dec}$을 이용하여 128bit의 암호문 C를 128bit 평문 P로 변환하는 복호화 함수 Decrypt Function으

표 1. LEA 규격
Table 1. The Standard of a LEA

Separate	N_b	N_k	N_r
LEA-128bit	16	16	24
LEA-192bit	16	24	28
LEA-256bit	16	32	32

www.dbpia.co.kr

로 구성된다.[9,10]

$$RK_i^{dec}(0 \le i \le (N_r - 1)) \quad (2)$$

다음 그림 5는 LEA에 대한 암호화 및 복호화의 과정을 도식화한 것이다.

암호화 스케줄 혹은 복호화 스케줄에 따라 라운드 지정한 수만큼 암호화 및 복호화를 수행하게 된다. 그리고 각 각의 암호화 스케줄과 복호화 스케줄은 동일한 비밀 키를 공유하고 있다.

이를 통해 서버와 클라이언트 간의 상호 보안 통신이 가능하게 된다. LEA는 암호화 및 복호화 스케줄링 외에도 별도로 함수가 존재하며, 각 각 Encrypt 함수와 Decrypt 함수로 나뉘며, 다음과 같은 과정을 통해 동작한다.[9,10]

· 암호화 함수

입력 = 128bit 평문 P, 192bit 라운드 Key RK_i^{enc}, 출력 = 128bit 암호문 C

$X_0 \leftarrow P$
for I = 0 to N_r-1 **do**
$X_{1+1} \leftarrow Round^{enc}(X_1, RK_i^{enc})$ (3)
end for
$C \leftarrow X_{Nr}$

· 복호화 함수

입력 = 128bit 암호문 C, 192bit 라운드 Key RK_i^{dec}, 출력 = 128bit 평문 P

$X_0 \leftarrow C$
for I = 0 to N_r-1 **do**
$X_{1+1} \leftarrow Round^{dec}(X_1, RK_i^{dec})$ (4)
end for
$P \leftarrow X_{Nr}$

2.3 LEA설계와 해석

본 논문에서는 해당 알고리즘을 통해 적용시킨 사용자에 따른 보안 시스템을 구축하기 위해 Arduino 개발 플랫폼 환경 기반으로 알고리즘을 재해석 하였다.

스마트 폭 인터페이스에 탑재한 사용자 보안은 CBC(Cipher Block Chaining) 운영모드를 아래의 그림 6과 같은 과정에 의해 설계하여 수행 하였다. CBC 운영모드는 Initial Vector(IV)를 사용하여 암호화 대상 블록을 체인 연속으로 연결시켜서 암호화 및 복호화를 처리하는 운영모드를 말한다.

CBC 운영모드를 스마트 폭 인터페이스에 대한 고유한 ID값과 사용자가 사전에 설정하고 입력한 비밀번호를 하나의 인증코드로 사용자에 따른 인식을 수

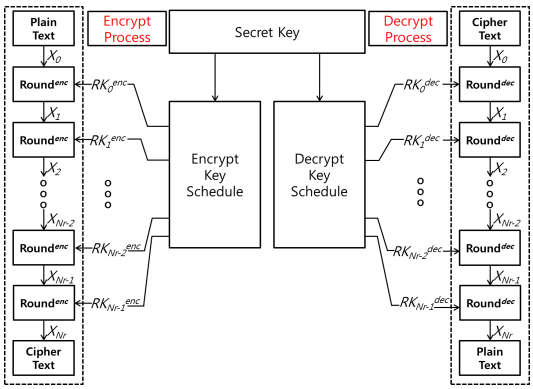

그림 5. LEA 암호화 및 복호화의 과정 도식화
Fig. 5. Diagram of LEA Encrypt and Decrypt Process

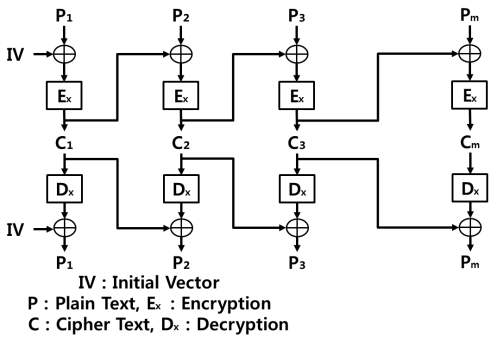

그림 6. LEA의 CBC 운영모드 암호화 및 복호화 과정
Fig. 6. CBC Operation Mode Encryption and Decryption Process of LEA

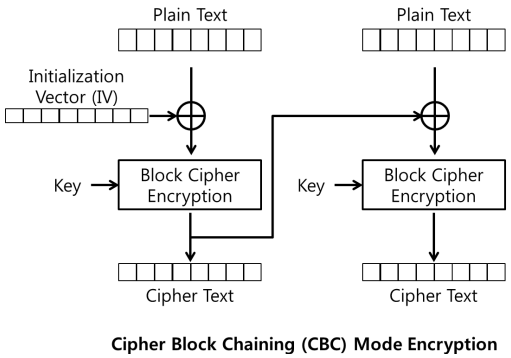

그림. 7. CBC 운영모드의 일부분
Fig. 7. Part of CBC Operation Mode

www.dbpia.co.kr

행하도록 구현하였으며, 이를 통해 다중 사용자가 동시에 접근을 하였을 경우에도 서로간의 충돌을 사전에 차단할 수 있게 된다.[11]

그림 6을 기반으로 설계와 동작은 다음 그림 7과 같다.

2.4 MTI 알고리즘 설계

스마트 퍽의 동작에 대한 사용자 중복영역을 피하기 위함과 사용자 인증의 의도적인 공격탐지 기법으로 사용되는 MTI 프로토콜은 Diffie-Hellman 방식의 키 사전 분배 방식을 개량하여 중간자 공격을 막을 수 있는 프로토콜로 'A로부터 B로'와 'B로부터 A로'의 두 개의 분리된 정보의 전송만이 있기 때문에 A와 B가 임의로 서명을 계산하는 것을 요구하지 않는다.

이 프로토콜을 2-패스(2-pass) 프로토콜이라고 한다.[12] 이 프로토콜의 환경은 Diffie-Hellman 키 사전 분배와 같이 소수 p 와 원시 근 A를 가정하며 키 동의에 사용되는 일회성 키들을 서명하여 교환하지 않고 사용자 레벨 키를 계산하는 방법으로, 기존 Diffie-Hellman 방식에서 가입자 A와 가입자 B가 항상 동일한 사용자 레벨 키를 가지게 되는 문제를 개선하였다.

본 논문에서 적용된 MTI 알고리즘 해석의 5단계는 아래의 표 2에 나타내었다.

표 2. MTI 알고리즘 해석
Table 2. Interpretation MTI algorithm

Step	Explanation
1 Step	Select a primitive element g on Z_p made of a large prime number p.
2 Step	user A and B is Calculate each public information $y_A \equiv g^{X_A} \bmod p$ and $y_B \equiv g^{X_B} \bmod p$.
3 Step	The calculated information is transmitted to KDC ID(A) and ID(B) together.
4 Step	Select each random number $R_A \in {}_R Z_{p-1}$ and $R_B \in {}_R Z_{p-1}$ then, calculate transmitted information $U_A \equiv g^{R_A} \bmod p$ and $U_B \equiv g^{R_B} \bmod p$ transmit to another user.
5 Step	When user A calculates $SK \equiv U_B{}^{X_A}{}_{yB^{R_A}} \bmod p$, and user B calculates $SK \equiv U_A{}^{X_B}{}_{yA^{R_B}} \bmod p$, The user level key $SK \equiv g^{X_A R_B + X_B R_A} \bmod p$ is shared.

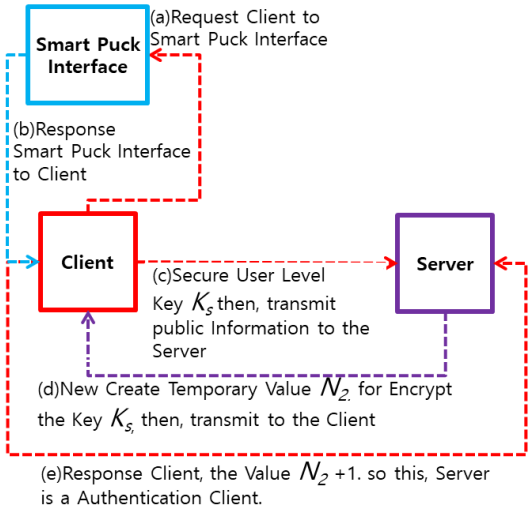

그림 8. 서버와 클라이언트의 보안 통신을 위한 키 레벨화 과정의 일부
Fig. 8. Part of Key Leveling Process for the Server and Client Security Communication

사용자 인증은 다수의 사용자가 알고 있는 마스터 비밀 키를 미리 공유하고 있다. 이 키를 사용하여 통신 쌍방 간에 필요한 단 기간의 사용자 레벨 키인 K_s를 배포할 뿐만 아니라, 이들 간에 상호 인증을 레벨화(Leveling)하여 설계할 수 있도록 한다. 클라이언트와 서버가 보안 통신을 위한 사용자 레벨에 따라 Key를 내려 받는 과정은 다음과 같다.

(a) 클라이언트 : 스마트 퍽 인터페이스에게 {클라이언트 ID, 서버 ID, cnonce 값 N_1}로 구성된 요청(Request)을 평문(Plain Text)으로 전송한다.(cnonce = Client Nonce)

(b) 스마트 퍽 : 다음 내용들을 마스터키(Mater Key)로 암호화(Encrypt)하여 클라이언트에게 응답한다.

- {사용자 레벨 Key K_s, Request, N_1}: 사용자 정보(User Information)
- {E_{kb}(사용자 레벨 Key K_s), 클라이언트 ID}: 레벨 설정(Level Setting)

(c) 클라이언트 : 사용자 레벨 Key K_s를 확보한다. 이어, 서버에게 공정 정보를 송신한다.

(d) 서버 : 클라이언트와 서버간의 공유 사용자 레벨 Key K_s를 확보한다. 또한 서버는 사용자 레벨을 암호화할 때 사용한 Key는 스마트 퍽 인터페이스만이 알고 있는 것이므로, 터치 테이블에 생성한 클라이언

www.dbpia.co.kr

트임을 믿게 된다. 이어, 클라이언트에게 자신이 새로 생성한 임시 값 N_2를 공유키 K_s로 암호화하여 다른 사용자에게 전송한다.

(e) 클라이언트 : N_2에 1을 더한 값으로 응답한다. 이렇게 함으로써, 서버가 클라이언트를 인증할 수 있도록 한다.

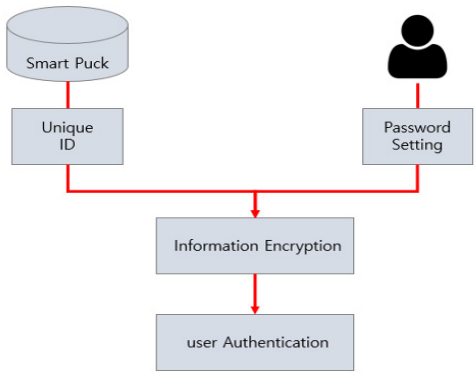

그림 9. 사용자 보안 인증 과정
Fig. 9. User Security Authentication Process

Ⅲ. 실 험

본 논문에서 해석한 스마트 퍽 인터페이스의 사용자에 대한 충돌, 중복 영역의 해석 그리고 의도적인 공격탐지 등의 기능에 대한 실험은 사용자와 스마트 퍽을 위한 보안과 인식의 전송 문자열을 8 바이트(Byte)의 IP 프래그먼트(Fragment)로 나누고, 이것을 대상 시스템으로 전송하여 대상 시스템이 IP 프래그먼트를 재조립하는 능력을 갖고 있는지를 결정한다.[13] 스마트 퍽으로 대상 사용자에게 적용되는 가상 프로토콜스택은 정확하게 대상 시스템과 같은 형식으로 프래그먼트를 처리한다.

다수사용자에 대한 스마트 퍽의 동작 프로토콜스택의 역할과 관계에 대한 기존 방법을 그림 10에 나타내고 있다. 이렇게 구성된 프로토콜스택은 펌웨어 종류가 서로 다른 시스템들에서 그림 10의 b와 같이 각각의 구성부분이 동일하게 적용된다.

그리고 스마트 퍽 정보의 대응전략을 위한 의도적인 공격탐지 시스템의 'Libpcap' 및 'Libnet' 라이브러리는 펌웨어의 특성을 따르지 않고, 클라이언트 데이터 싱크는 스마트 퍽 센싱으로 구성되어 환경이 다른 시스템과 독립적으로 작동한다.[14,15]

따라서 본 논문에서 설계한 다수 사용자를 위한 스마트 퍽의 프로토콜 스택은 다양한 콘텐츠 특성에 영향 없이 독립적으로 구성되고 연동제어 시뮬레이션을 수행하였다. 본 논문에 대한 실험을 위한 제약 조건으로서는 네트워크 환경에 대한 제약 조건으로, 동일한 네트워크 대역폭 내에서의 테스트를 위해 같은 망을 사용하는 환경을 구축한 뒤 실험을 진행한다.

스마트 퍽 인터페이스는 내장된 Wifi 모듈을 이용하여 네트워크 통신을 하므로, 이에 대해 같은 공간상에서의 동일한 망을 사용해야 정상적인 통신이 가능하다. 예컨대, Wifi 환경을 이용하기 위해서 공유기와 같은 장비가 추가적으로 필요하며, 공유기를 통해 분배되는 IP Address를 스마트 퍽 인터페이스에 할당하여주고, 이를 통해 멀티터치 테이블 및 서버와의 통신을 행하게 된다.

그림 11은 4 명의 사용자를 위해 스마트 퍽 4개를 활용한 LEA의 CBC 방법과 MTI 방법의 보안엔진에서 생성하는 경보의 전체 부하량이 50%에서 90%까지에 대한 스마트 퍽을 이용한 전송 성능을 평가한 것이다.[16]

LEA 방법과 MTI 방법이 병행한 보안 엔진에서 생

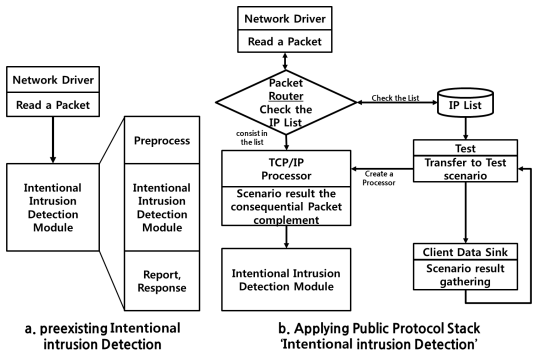

그림 10. 스마트 퍽의 프로토콜스택 적용 전후 동작 순서
Fig. 10. Before and after application of smart puck protocol stack of Operation sequences

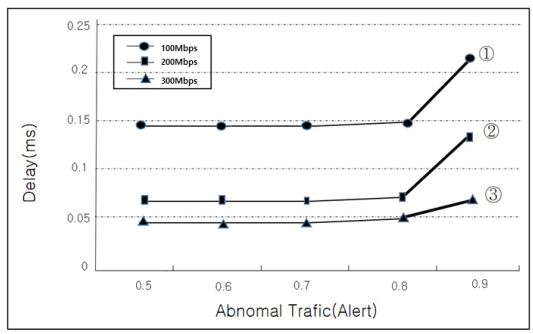

그림 11. 의도적인 공격을 이용한 정보지연
Fig. 11. Information delay using intentional attack

www.dbpia.co.kr

성한 경보를 주 프로세서의 대응 능력에 따른 정보 지연으로 해석하였다. 정보의 양에 따라 대응 유닛의 100Mbps 처리 속도에서 그림 11의 ①과②는 심각한 지연을 나타내고 있다.

스마트 펙의 보안에서 생성한 정보의 전달을 주 프로세서로 전송할 때, 그 대응 능력을 수행의 원활한 평균 트래픽이 0.8을 넘을 경우는 전송지연이 급격함을 나타낸다. 따라서 정보의 지연과 성능은 스마트 펙의 사용자의 수에 대한 대응 처리 속도와 가장 밀접하게 연관된 것으로 분석되어 이에 대한 대응능력으로 세그먼트 크기의 조정으로 상쇄할 수 있다.

그림 12와 그림 13은 시뮬레이션 모델이 보안엔진에서 생성하는 경보의 전체 부하량이 50%에서 150%까지에 대하여 대응 유닛 300Mbps에서 스마트 펙 들의 전송 시, 세그먼트 수에 따른 지연과 손실을 나타낸다.[17] 여기서 세그먼트의 수가 작을수록 지연은 감소하는 반면 손실은 증가하는 경향을 보인다. 그러나 손실 성능은 세그먼트의 크기에 따라 그림 11에서 평균 트래픽 0.8을 기점으로 전송지연이 증대되었으나 그림 12와 그림 13에서는 평균 트래픽 1.0을 기점으로 전송지연 손실이 향상됨을 알 수 있다.

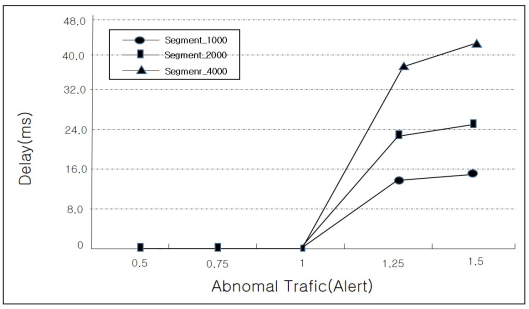

그림 12. 세그먼트 크기에 따른 정보 지연
Fig. 12. Delay of information according to segment size

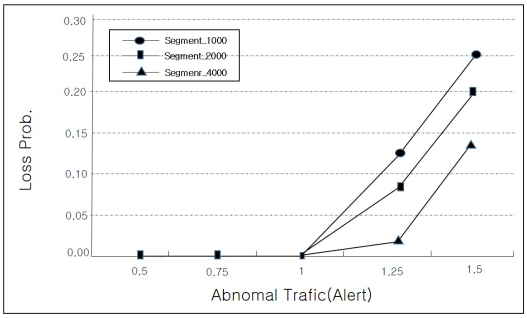

그림 13. 세그먼트 크기에 따른 정보 손실
Fig. 13. Loss of information according to segment size

Ⅳ. 결 론

본 논문에서는 차세대 인터페이스인 스마트 펙 환경과 TUI방식 환경에 최적화되도록 LEA 암호화 알고리즘과 MTI 인증 방법을 적용하여 다수의 사용자에 따른 인증 모듈을 설계하였다. 스마트 펙의 고유한 ID값과 사용자가 설정한 비밀번호를 병합하여 MTI 알고리즘 방식의 새로운 인증 키 값을 생성하고 또 해당 인증 키 값을 통해 스마트 펙 인터페이스를 이용하는 다수의 사용자에게 편의성을 제공할 수 있었다.

이는 멀티 터치 테이블 상에 최대 4 명의 사용자에 대한 스마트 펙을 에 올려놓아도 타 사용자와의 접근 시 충돌되지 않았다. 이로써 멀티 회의 시스템이나 멀티 게임 콘텐츠 등 기존의 TUI 방식의 환경에서 다중 사용자간의 인터페이스가 충돌되어 발생하는 문제를 해소하였으며, 이에 따라 동시에 다수의 사용자들이 상호간에 정보를 주고받는 형태가 좀 더 자유롭게 수행하였다.

향후의 연구는 새로운 인터페이스 장치인 스마트 펙에 대한 향상된 성능과 LEA 암호화 알고리즘의 최적화된 라운딩, 체인징 과정의 간략화와 MTI과정의 간소화 등으로 환경으로 제공하여 멀티 터치 테이블 서비스에서 보다 효율적인 인증 처리와 실시간 데이터 송수신을 위한 빠른 연산처리가 되도록 개선하는 연구가 있다.

References

[1] P. Ryong Kim, "Analysis of the market and industry structure on the information security industry," *J. KICS*, vol. 43, no. 1, pp. 191-200, Jan. 2018.

[2] D. J. Hong, et al., "LEA : A 128-bit Block Cipher for Fast Encryption on Common Processors," *Int. Wksp Inf. Secur. Appl.*, pp. 3-27, Aug. 2014.

[3] S. H. Bak, E. S. Kim, J. B. Lee, and H. M. Lee, "Arduino-based tangible user interfaces smart puck systems," *J. Korea Multimedia Soc.*, vol. 19, no. 2, pp. 334-343, Feb. 2016.

[4] S. H. Bak, E. S. Kim, and H. M. Lee, "A smart puck system using tangible interfaces," in *Proc. The Korea Contents Assoc. Conf. 2015*, pp. 341-342, Silla University, Busan Metropolitan City, Korea, May 2015.

www.dbpia.co.kr

[5] L. H. Kim, H, C. Cho, S. H. Park, “Smart puck system : Tangible interface for physical manipulation of digital information,” *Korean Inst. Inf. Sci. Eng.*, vol. 13, no. 4, pp. 226-230, Aug. 2007.

[6] J. M. Jeong, H. J. Yang, and S. H. Kim, “Multi-modal sense based interface for augmented reality in table top display,” *J. Korea Multimedia Soc.*, vol. 12, no. 5, pp. 708-716, May 2009.

[7] S. Y. Kang and J. H. Kim, “Module design of user security authentication for smart puck interface with gesture sensing,” in *Proc. KICS Int. Conf. 2017*, pp. 333-334, Kyungpook National University, Daegu Metropolitan City, Korea, Nov. 2017.

[8] G. T. Park, H. J. Han, and J. H. Lee, “Design and implementation of lightweight encryption algorithm on OpenSSL,” *J. Korean Inst. Commun. and Inf. Sci.*, vol. 39, no. 12, pp. 822-830, Dec. 2014.

[9] TTAK, *128-Bit Block Cipher LEA*(2013), Retrieved Jan, 2018, from http://www.tta.or.kr.

[10] TTAK, *Modes of Operation for the 128-Bit Block Cipher LEA*(2014), Retrieved Jan. 2018, from http://www.tta.or.kr.

[11] NSR, *128Bit Block Cipher LEA Specification*,” Retrieved Jan. 2018, from https://seed.kisa.or.kr.

[12] Behroun A. Forouzan, *Cryptography and Network SEcurity*, pp. 467-471, McGrow-Hill, 2012.

[13] C. C. Michael and A. Ghosh, “Simple, state-based approaches to program-based anomaly detection,” *ACM Trans. Inf. and Syst. Secur.*, vol. 5, no. 3, pp. 212-217, Mar. 2002.

[14] J. Barrus and Neil C. Rowe. “A distributed autonomous agent network- intrusion detection and response system,” in *Proc. Command and Control Res. and Technol. Symp.*, pp. 577-586, Monterey, CA, Jun. 2008.

[15] J. H. Lim, et al., “A closed-loop approach for improving the wellness of low income elders at home using game consoles,” *IEEE Commun. Mag.*, vol. 50, no. 1, pp. 44-51, Jan. 2012.

[16] J. Ko, et al., “Connecting low-power and lossy networks to the internet,” *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 96-101, Apr. 2011.

[17] A. Perrig, D. Song, R. Canetti, J. D. Tyger, and B. Briscoe, *Timed Efficient Strem Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction*, RFC 4082, Jun. 2005.

강 시 영 (Si-Young Kang)

2017년 8월 : 국립한밭대학교 컴퓨터공학과 졸업(학사)
2018년 3월~현재 : 경북대학교 전자공학부 재학(석사과정)
<관심분야> IoT Security, Deep learning, AI, Big Data Information Security, LEA

김 정 호 (Jeong-Ho Kim)

1980년 2월 : 경북대학교 전자공학과 졸업(공학사)
1983년 2월 : 경북대학교 대학원 전자공학과 졸업(공학석사)
1994년 2월 : 단국대학교 대학원 전자공학과 졸업(공학박사)
1983년3월~1996년 한국전자통신 연구원(실장, 책임연구원)
1989년 8월 : 정보처리기술사
1990년 8월 : 산업계측제어기술사
1991년 12월 : 정보통신기술사
1996년 3월~현재 : 한밭대학교 컴퓨터공학과 교수
<관심분야> 네트워크와 데이터통신, 정보보호

www.dbpia.co.kr