Regular paper | Journal of the KIECS. pp. 1143-1150, vol. 12, no. 6, Dec. 31 2017, t. 86, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2017.12.6.1143

개방형 무료 Wi-Fi의 해킹위험 사전경고 표시

정병문* · 이태희* · 이영식* · 최철재**

Method of Forewarning Display for Hacking Risk in the Open Wi-Fi

Byung-Moon Jeong* · Tae-Hee Lee* · Young-Sik Lee* · Chul-Jae Choi**

요 약

본 논문은 개방형 무료 Wi-Fi 접근영역에서 비전문가들을 위한 사용자 경험인 UX(: User Experience) 개념 차원에서 해킹위험 경고표시 방법을 제안하였다. 캡처에 의해 올라온 AP들의 위험성에 따라 색깔로 구별하며 선택 된 AP에 대하여 사용 전에 해킹의 위험을 팝업창으로 경고문을 제공하는 앱을 개발하였다.

ABSTRACT

In this paper, we proposed a method to display a hazard warning of hacking in the UX(: User Experience) concept level for non experts in the open Wi-Fi access area. According to the dangers of the AP raised by capture, we developed an application that provides a warning pop-up on the danger of hacking before using for APs that are distinguished by color and selected.

키워드

Wi-Fi, Wireless Internet, Hacking Danger Display, Access Point
Wi-Fi, 무선 인터넷, 해킹 위험 표시, AP

Ⅰ. 서 론

개방형 무료 Wi-Fi는 매우 매력적이다. 또 다른 이름의 공공 Wi-Fi는 편리한 무선인터넷 접속환경을 제공하면서 공짜라서 비용부담이 없다. 그만큼 편리성과 접근성 면에서 획기적 변화이다. '언제 어디서나'로 대변되는 유비쿼터스시대[1]를 실현하는 핵심적 기술 중에 하나일 것이다. 모바일 정보기기 사용자의 요구중심의 환경에 필수적이다[2-4].

그러나 이러한 개방형 무료 Wi-Fi는 편리함의 순기능 이면에 해킹위험으로 인한 역기능적 위협요인에 항상 노출되어있다. 그림 1과 같이 개방형 무료 Wi-Fi는 여러 사람이 해당 영역에서 동일한 무선접속장치(AP: Access Point)를 사용하기 때문에 다른 사람의 의한 접근통제가 취약하다[1]. 그러므로 개방형 무료 Wi-Fi 네트워크 영역에서 비밀번호 크랙(password crack) 시도가 있을 경우 허술한 조합으로 구성된 쉬운 비밀번호를 지정하여 사용하는 이용자는 사이버 범죄의 표적대상이 된다.

1) http://www.connectone.com/?page_id=3837

* 경동대학교 정보보안학과(jbm2112@naver.com, thlee@kduniv.ac.kr, young@kduniv.ac.kr)
** 교신저자 : 경동대학교 정보보안학과
· 접 수 일 : 2017. 09. 21
· 수정완료일 : 2017. 11. 02
· 게재확정일 : 2017. 12. 15
· Received : Sep 21, 2017, Revised : Nov 02, 2017, Accepted : Dec 15, 2017
· Corresponding Author : Chul-Jae Choi
Dept. of Cyber Security for Information, Kyungdong University,
Email : cj-choi@kduniv.ac.kr

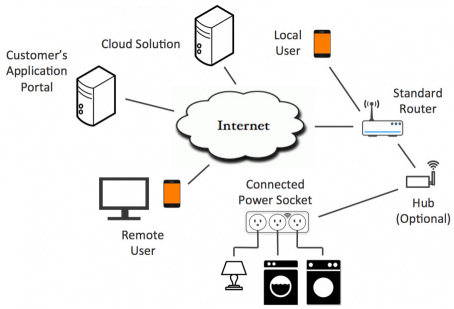


그림 1. 개방형 무료 Wi-Fi 환경
Fig. 1 Open Wi-Fi environment

최근, 개방형 무료 Wi-Fi 서비스 영역이 급속하게 무한대로 확산되고 있으나 이에 대한 인식부족과 기술적으로도 사이버범죄의 악용방지를 위한 대비책은 부족하다. 어쩌면 개인적인 책임 하에 방임되고 있다고 봐도 과언이 아니다[5].

따라서 본 논문에서는 개방형 무료 Wi-Fi에 사용되는 암호화 방식 및 암호화 기술 공격에 대해 알아보고, 무료 Wi-Fi 해킹 사례를 분석한 뒤 해결방안으로 개방형 무료 Wi-Fi 영역에 스캔으로 올라온 AP들을 위험성 여부에 따라 색깔로 구별하며 선택된 아이템에 대해 사용 전에 해킹의 위험을 팝업창 형식으로 경고문을 제공하는 앱을 개발하였다.

II. 해킹 취약점과 사례

2.1 무선암호화 방식

무선암호화의 일반적 프로토콜에는 표 1과 같이 WEP, WPA, WPA2가 있다[6].

표 1. 무선 암호화 방식
Table 1. Wireless encryption method

	WEP	WPA	WPA2
Authentication	Universal method, using preshared secret key	Using shared secret key and authentication server	Using shared secret key and authentication server
Encryption	Use fixed encryption key Use RC4 algorithm	Dynamic change of encryption key Use RC4 algorithm	Dynamic change of encryption key Use AES block
Security	Exposure of risk of hacking, Leave gradually	Use RC4 that is safer or incomplete than WEP	It provides the most powerful security function

세 프로토콜은 가장 많이 사용되는 무선암호화 프로토콜이다. 무선 랜발견으로 표준선택에서 제외되었다. 이후 WPA, WPA2로 대체되어 사용되었으나, 현재는 WPA2를 사용하도록 권고한다.

2.2 무선공유기 공격

2.2.1 WEP 크래킹

WEP(: Wired Equivalent Privacy)은 널리 사용되는 Wi-Fi 보안알고리즘으로 IV(: Initial Vector)와 Key 값을 이용하며 스트림 암호화 기법인 RC4을 통해 평문을 암호화한다. 취약점 개선노력이 있지만, 2001년 치명적 취약점 발견으로 비영리 Wi-Fi기술 인증기관인 Wi-Fi Allicance에서 2004년 공식적으로 WEP 방식을 퇴출시켰다.

2.2.2 WPA/WPA2 크래킹

WPA는 Wi-Fi Allicance에서 WEP의 취약점 대체하기 위한 표준이다. TKIP(: Temporal Key Integrity Protocol)이 추가되어 이후 AES(: Advanced Encryption Standard)로 대체되었지만 취약점이 여전히 존재한다. WPA2는 AES가 기본알고리즘이며 CCMP방식이 TKIP방식을 대체하여 결합한다. 따라서 WPA2는 기업의 네트워크가 아닌 개인용 네트워크에는 안전성 방식으로 보고 있다. 물론 WPA2 역시 크랙(Crack) 위험은 있으나[7-8]. 대규모 기업수준의 보안요구가 아니면 WPA/WPA2-PSK 정도의 보안수준 유지로도 충분할 것으로 판단하고 있다[9].

2.3 개방형 Wi-Fi의 공격시나리오

그러나 무선암호화 프로토콜의 기술적 개선에도 불구하고 현실적으로 여전히 개방형 무료 Wi-Fi의 사용에는 해킹의 위험이 도사리고 있다. 이로 인해 많은 정보가 유출되고 기기들이 감염되고 있는 것이다. 임의로 서울 모지역의 카페, 식당 등 각종 영업소의 개방형 무료 공유기의 보안 설정을 조사한 결과 약 10장소 중 8장소가 취약한 공유기를 소유하고 있는 것으로 파악되었다.

공격시나리오의 접근절차는 ① 공격자가 게시판에 <공격자가 제작한 악성사이트로 접속 시 연결되어있는 공유기의 DNS를 변조시키는 코드>를 작성 및

업로드 ② 사용자가 개방형 무료 Wi-Fi 접속 ③ 출처 불분명, 자극적 게시물 열람 ④ 개방형 무료 공유기 침투 및 DNS 변조 ⑤ 이후 DNS IP가 변조된 공유기를 통해 인터넷 접속 시 악성사이트로 강제 이동 순서로 진행되며 그림 2와 같다.

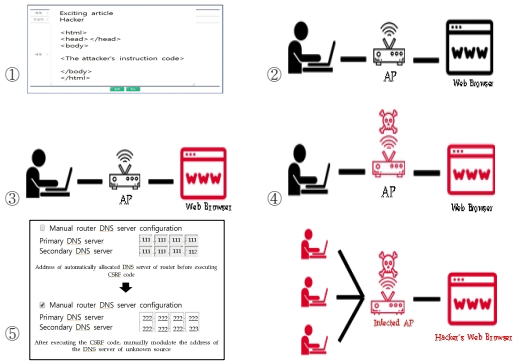


그림 2. 공격시나리오의 접근절차
Fig. 2 Access procedure for attack scenario

2.4 공격시나리오의 취약점 원인

공격시나리오에서 취약점의 원인은 크게 취약한 공유기와 모바일 사용자의 보안설정 인식부족을 들 수 있다. 취약한 공유기란 그림 3과 같이 공유기 관리자 로그인 암호 미설정, 공유기 DNS 자동 설정으로 설정되어 있는 경우 등이라고 할 수 있다.

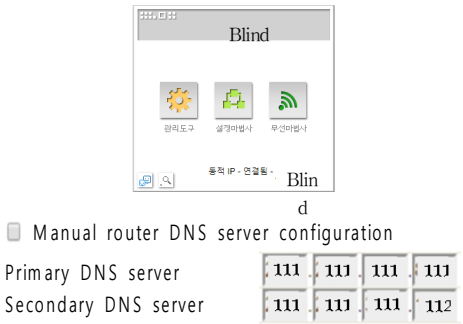


그림 3. 취약한 공유기
Fig. 3 Vulnerable router

모바일 사용자의 보안설정 인식부족은 [Wi-Fi에 연결] - [Wi-Fi 설정 창] - [연결된 Wi-Fi 상세정보 보기] - [보안 설정 부분 확인] - [보안 설정 안함, WEP, 암호 미설정일 경우 사용 한하는 것을 권장] 등의 방법으로 해소될 수 있다.

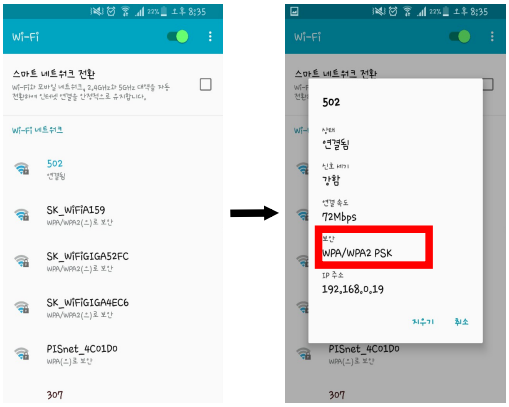


그림 4. Wi-Fi의 보안설정 확인
Fig. 4 Checking for security setting of Wi-Fi

III. 해킹위험 사전경고 표시

3.1 시스템 블록다이어그램

모든 아래 그림 5는 개방형 Wi-Fi에서 해킹위험 경고표시를 위한 전반적인 블록다이어그램이다. Main 모듈은 암호 유무 판단과 보안 방식을 판별하는 기능을 하고, Sub로 표시된 영역에 속하는 프로그램 모듈들은 리스트 안에 있는 각각의 아이템을 표시하는 데이터 상태에 따라서 Wi-Fi 영역에 접근한 사용자의 모바일에 각각 디스플레이 해준다.

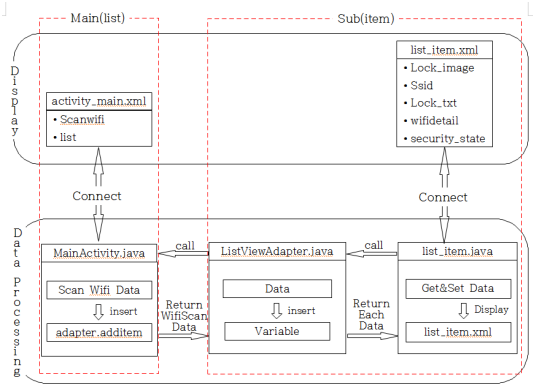


그림 5. 블록 다이어그램
Fig. 5 System block diagram

3.2. 프로그램 모듈

3.2.1. 암호유무판단

사용자가 특정 영역의 위치에 접근했을 때 캡처된 AP가 인증절차를 요구하는지를 판별하는 프로그램 모듈이다. 만일 보안이 WPA 방식이 아니면 "Open" 상태이고, Lock_img는 "Unlock" 이미지를 표시한다.

```
if(!wifiList.get(i).capabilities.contains("WPA")) {
Locking_State = "Open";
Lock_image =ContextCompat.getDrawable(MainActivity.this,
R.drawable.unlock);
}
else{
Locking_State = "Lock";
Lock_image =ContextCompat.getDrawable(MainActivity.this,
R.drawable.lock);
}
```

그림 6. 암호의 유무판단
Fig. 6 Determine the presence or absence of a password

3.3.2 보안형식에 따른 안전도 표시

사용자가 특정 영역의 위치에 접근했을 때 캡처된 AP의 보안방식에 따라 WPA, WPA2 이면서 비밀번호가 설정되어 있는지 아닌지에 따라 그림 7의 Security_state를 list에 보여준다.

```
if(wifiList.get(i).capabilities.contains("WPA-") &&
wifiList.get(i).capabilities.contains("WPA2-") &&
Locking_State.contains("Lock")){
Security_state = "Safety";
}
else if(wifiList.get(i).capabilities.contains("WPA-") ||
wifiList.get(i).capabilities.contains("WPA2-") &&
Locking_State.contains("Lock")){
Security_state = "Normal";
}
else {
Security_state = "Vulnerable";
}
```

그림 7. Security_상태 리스트
Fig. 7 Security_state List

3.3.3 list_item.java

그림 8은 그림 6와 그림 7에서 처리한 데이터에 따라 list_item.xml에 출력할 java 프로그램 모듈이다. 여기서 set 메소드는 get 메소드에서 받아온 데이터로써 그림 9의 상태를 설정하는 것이며, get 메소드는 mainactivity.java에서 처리된 lock_image, ssid, locking, wifidetail, Security_state의 데이터를 list_item.xml로 받아오는 메소드이다.

```
import android.graphics.drawable.Drawable;
public class list_item {
private  Drawable Lock_image;
private String Ssid;
private String Locking;
private String Wifidetail;
private String Security_state;
public void setLock_image(Drawable icon){
Lock_image = icon;
}
public void setSsid(String SSID){
Ssid = SSID;
}
public void setLock(String locking){
Locking = locking;
}
public void setWifidetail(String wifidetail){
Wifidetail = wifidetail;
}
public void setSecurity_state(String security_state){
Security_state = security_state;}
public Drawable getLock_image(){
return this.Lock_image;
}
public String getSsid() {
return Ssid;
}
public String getLocking(){
return Locking;
}
public String getWifidetail() {
return Wifidetail;
}
public String getSecurity_state(){
return Security_state;
}
}
```

그림 8. list_item.xml 출력처리
Fig. 8 Processing of list_item.xml

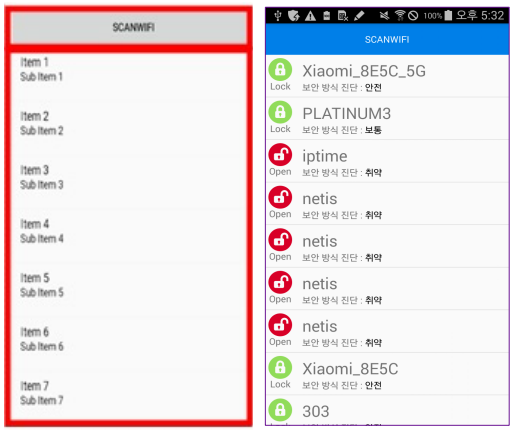
3.3.4 list_item.xml

화면표기에서 Lock_image는 그림 9와 같이 자물쇠 모양으로 Lock, Unlock(Open Close) 상태를 표시한다. SSID는 무선공유기 또는 AP의 고유 식별자이다. Lock_txt와 Security_state로 구성되어 있다. 그림 10은 처리모듈이고, 그림 11은 처리화면이다.

그림 9. AP Item 디자인
Fig. 9 AP Item design

```
adapter.addItem(imageView, SSID, Locking_State,
"₩nSecurity_method₩n" + Security + "₩n₩nSignal
strength(RSSI)₩n" + Level_string + " (" + Level + " dBm)"
+ "₩n₩nMac Address(Physical address)₩n" + BSSID,
Security_state);
}
```

그림 10. 스캔된 AP 정보처리
Fig. 10 Information process of the scanned AP



(a) 초기화면 디자인 (b) 스캔된 AP List
(a) Initial screen (b) Scanned AP List

그림 11. 디자인과 초기 스캔
Fig. 11 Design and first scan

3.3.5 AP 상세정보 출력 Dialog

스캔된 AP를 터치 시 해당 AP의 보안방식, 신소세기, 물리주소를 상세하기 표시하는 다이얼로그를 그림 13과 같이 팝업한다. 안전성 확인버튼을 터치 시 설정되어 있는 보안방식에 따라 비전문가를 향한 그림 11과 같은 경고성 Dialog 또는 안전성 Dialog를 팝업한다. 경고성 또는 안전성 Dialog를 숙지한 사용자는 OK 버튼을 터치 시 그림 12와 같이 해당 AP에 연결한다.

```
list_item item = (list_item)list_item.getItemAtPosition(i);
final AlertDialog.Builder wifidetail = new
AlertDialog.Builder(MainActivity.this);
wifidetail.setTitle(item.getSsid());
wifidetail.setMessage(item.getWifidetail());
wifidetail.setNegativeButton("Safety confirmation", new
DialogInterface.OnClickListener() {
public void onClick(DialogInterface dialog, int which) {
dialog_Message.show();
}
});
wifidetail.setPositiveButton("Cancel", new
DialogInterface.OnClickListener() {
public void onClick(DialogInterface dialog, int which) {
dialog.cancel();
}
});
```

그림 12. 스캔된 AP 상세정보 처리
Fig. 12 Detail Info of Scanned AP processing

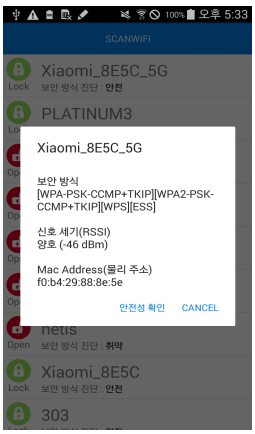
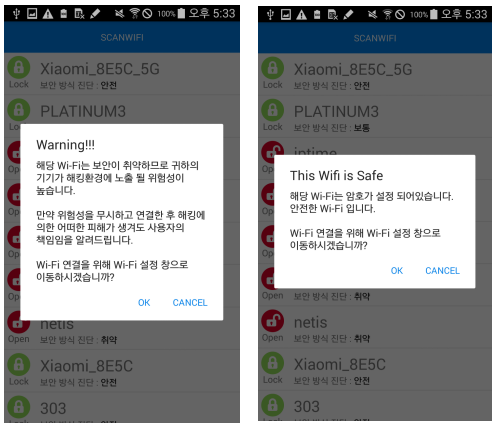


그림 13. 스캔된 AP 상세정보 출력
Fig. 13 Detailed information output of scanned AP



(a) 경고성 Dialog (b) 안전성 Dialog
(a) Warning Dialog (b) SafetyDialog

그림 14. 경고성 및 안전성 Dialog
Fig. 14 Warning and Safety Dialog

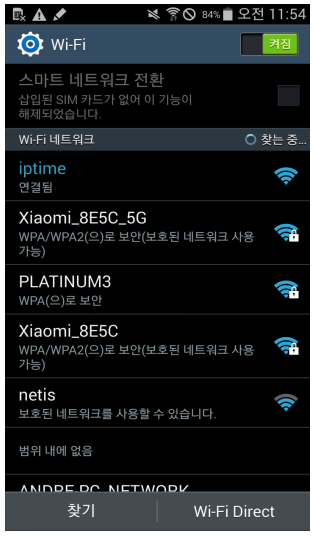


그림 15. Wi-Fi 연결
Fig. 15 Wi-Fi connection

Ⅳ. 결 론

유비쿼터스시대의 보편적 서비스로 등장한 개방형 무료 Wi-Fi가 편리함과 공짜라는 이유로 이용자와 응용분야 가파르게 증가하고 있다[10]. 그러나 개방형 Wi-Fi 사용에는 해킹의 위험성 상존하고 있다. 이를 이용한 금융거래나 개인정보를 사용하는 서비스에 안전을 보장받을 수 없다.

따라서 본 논문에서는 개방형 무료 Wi-Fi에 사용되는 암호화 방식 및 암호화 기술 공격에 대해 알아보고, 개방형 무료 Wi-Fi 해킹 사례를 분석한 뒤 해결방안으로, Wi-Fi 영역에 스캔으로 올라온 AP들을 위험성 여부에 따라 색깔로 구별하며 선택된 AP에 대해 사용 전에 해킹위험을 팝업창으로 경고문을 제공하는 앱을 개발하였다.

향후 경고표시방법을 서버에서 구현하는 방법과 사용자경험기술 개발개념을 도입한 진화된 안전성 확보방안에 대한 연구가 필요할 것으로 판단된다.

감사의 글

본 논문은 2017년도 한국전자통신학회 봄철 종합학술대회 우수논문의 확장본입니다.

Reference

[1] C. Lee, “Design by Improved Energy Efficiency MAC Protocol based on Wireless Sensor Networks,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 3, 2017, pp. 439-444.

[2] S. Jung and C. Sim, “A Study on a Wind Turbine Data Logger System based on WiFi for Meteorological Resource Measurement,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 10, no. 1, 2015, pp. 55-64.

[3] D. Choi, “Evaluation of VoIP Capacity for IEEE802.11b WiFi Environment under Voice Coding Methods,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 7, no. 2, 2012, pp. 243-248.

[4] S. Cho, "Performance Enhancement of Trilateration Localization using Wi-Fi RSSI Data,” *Telecommunication Review*, vol. 25, no. 1, 2015. pp. 134-144.

[5] S. Jeong and H. Shin, “Method and Apparatus for indoor position Measurement,” *J. of the Korea Institute of*

Electronic Communication Sciences, vol. 6, no. 6, 2011, pp. 903-908.
[6] H. Bae, M. Kim, S. Song, S. Lee, and Y. Chang, "Security Attack Analysis for Wireless Router and Free Wi-Fi Hacking Solutions," *J. of the Convergence on Culture Technology (JCCT),* vol. 2, no. 4, 2016, pp. 65-70.
[7] W. Jung, J. Lee, and C. Lee, "Security Vulnerability and Cracking Case of Wireless routers," *Proc. of the 2016 Winter Conf. on The Korea Institute of Communication and Information Sciences*, Jeongseon, Korea, January, 2016, pp. 665-667.
[8] S. Kwon and D. Park, "A Study of Wired and wireless VoIP vulnerability analysis and hacking attacks and security," *J. of Communications and Networks,* vol. 16, no. 4, 2012, pp. 737-744.
[9] B. Dagar and N. Goyal, "Integrating Enhanced Security Measures in WEP/WPA/WPA2-PSK," *Int. J. of Innovative Research in Computer and Communication Engineering*, vol. 4, issue 2, Feb. 2016, pp. 1240-1245.
[10] Y. Lee, "Development of Smart Garden Control System Using Probabilistic Filter Algorithm," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 12, no. 03, 2017, pp. 465-470.

저자 소개

정병문(Byung-Moon Jeong)

2014년 경동대학교 정보보안학과 입학
2017년 경동대학교 정보보안학과 4학년 재학중
※ 관심분야 : 모바일 보안, 웹서버보안, 컴퓨터교육

이태희(Tae-Hee Lee)

1995년 청주대학교 전자계산학과 졸업(공학사)
1999년 청주대학교 대학원 전자계산학과 졸업(공학석사)
2004년 청주대학교 대학원 전산정보공학과 졸업(공학박사)
2001년~2013 동우대학 컴퓨터학부 교수
2013년~현재 경동대학교 정보보안학과 교수
※ 관심분야 : 로보틱스, 원격제어

이영식(Young-Sik Lee)

1986년 한국항공대학교 통신정보공학과 졸업(공학사)
1996년 경희대학교 산업정보대학원 정보통신학과 졸업(공학석사)
2004년 관동대학교 대학원 전자통신공학과 졸업(공학박사)
1985년~1992 삼성전자 통신종합연구소
1992년~1995 경복대학 전자계산과 전임강사
1997년~현재 경동대학교 정보보안학과 교수
※ 관심분야 : 전자통신공학, 사이버범죄론

최철재(Chul-Jae Choi)

1983년 광운대학교 전자계산학과 졸업(이학사)
1987년 한양대학교 산업대학원 전자계산학전공 졸업(공학석사)
2000년 강원대학교 컴퓨터과학과 졸업(이학박사)
1988년~현재 경동대학교 정보보안학과 교수
2015년~2016 경동대학교 평생교육원장
※ 관심분야 : 데이터처리, 영상처리, 웹보안