2018년 한국정보보호학회 동계학술대회(CISC-W' 18)

DQ-Net : 동적 QR 코드 기반 Wi-Fi 인증 메커니즘

양유진, 임정현, 최정은, 서화정*1)

한성대학교 IT융합공학부

DQ-Net : Dynamic QR code-based Wi-Fi authentication mechanism

YuJin Yang, JeongHyun Lim, JeongEun Choi, HwaJeong Seo*

Division of IT Convergence Engineering, Hansung University.

요 약

무선 네트워크 기술인 Wi-Fi(Wireless Fidelity) 사용 시, 대부분의 이용자들이 SSID(Service Set Identifier)의 기본값을 그대로 사용함으로써, 관련된 정보를 알고 있는 해커들에게 공격당할 가능성이 높아진다. 번거로움 때문에 초기의 비밀번호를 그대로 사용하면, 비밀번호를 공유하는 사람이 늘어나면서 시간이 지날수록 보안성이 떨어지는 문제점이 발생한다. 본 논문에서는 이러한 보안 취약점 해결과 동시에 사용 편의성을 향상시키는 방법을 제안한다.

I. 서론

현재 Wi-Fi가 널리 사용되고 있음에도 불구하고 Wi-Fi 보안에 대한 사람들의 관심은 턱없이 부족하다. 그렇기에 사람들은 암호가 설정 되어 있지 않은 Wi-Fi를 아무 의심 없이 사용한다. 이는 나쁜 의도를 가진 사용자에게 해킹당할 위험성을 증가시킨다.[5] 또한 암호가 설정되어 있더라도 주기적으로 변경하지 않기에 보안성은 점차 취약해진다.

스마트폰 이용 확대와 함께 QR 코드(Quick Response Codes) 스캐너 프로그램이 다양하게 개발되면서 QR 코드의 활용이 늘고 있다. 하지만 QR 코드는 사람이 인식할 수 없기 때문에 안전성 검증이 쉽지 않고, 누군가 악의적으로 변경할 가능성이 있다. [2]

본 논문에서는 강원대학교 이남세 석사가 제안한 PS-Net[1](개인별 보안 Wi-Fi 네트워크)에서 아이디어를 착안하였다. PS-Net에 상업적 측면을 추가하고, 보안을 더욱 강화하는 방안을 제시한다. 사용자 중심 네트워크로 동적 QR 코드를 이용함으로써 악의적으로 QR 코드를 변경하는 것을 방지할 수 있다.

1.1 관련 연구

Fig. 1. Composition of Ps-Net using QR codes

사용자는 정보를 입력하여 보안을 설정함으로써 사용자 맞춤 가상 Wi-Fi 네트워크를 형성할 수 있다. 우선 QR 코드화한 AP(Access Point) 공개키(public key)를 기기로 인식하여 키를 취득하고, 어플을 이용하여 사용자로부터 SSID와 비밀번호를 입력받는다. 이후 AP 공개키와 입력받은 정보를 AP에 전달한다. 이 정보를 AP에 전송하기 위해서 public channel이 사용되는데, 이는 보안에 취약하다. 따라서 Fig. 1의 ③에서 RSA 암호화 알고리즘을 사용해 암호화를 해야 한다. 이후 AP는 개인키(private key)를 사용하여 암호화된 정보를 해독한다. 복호화된 정보를 이용하여 새로운 가상 AP를 생성하고, 사용자는 가상 Wi-Fi 네트워크를 이용할 수 있게 된다.

* 교신저자 : hwajeong84@gmail.com

II. 본론

기존의 Wi-Fi 인증 방식은 네트워크에 설정된 비밀번호를 입력하는 '네트워크 중심 인증 방식'인 반면에, PS-Net과 DQ-Net은 '사용자 중심 인증 방식'으로, 사용자가 SSID와 암호를 설정하여 네트워크를 사용한다. 하지만 DQ-Net은 PS-Net과 달리 어플을 설치하지 않고 public channel인 일회성 사이트를 제공한다. 이 사이트는 인증만을 위해 사용하는 것이기 때문에 용도를 다하면 자동으로 소멸한다. 또, PS-Net은 AP 기기 근처에 종이로 출력된 QR 코드를 공개하는 반면, DQ-Net은 디스플레이가 설치된 AP 기기 화면에서 QR 코드를 제공한다.

2.1 DQ-Net 구성 제안

Fig. 2. Suggestions of DQ-Net composition
① Output dynamic QR codes to the display
② Scan the QR codes with the Smart Phone
→ Obtain AP public key & Link to disposable page
③ Enter the information(SSID, P/W) at the site AP via public channel
④ Decode the data with AP private key
→ Create and provide virtual Wi-Fi Networks
→ Cease to exist the page

Fig. 2는 동적 QR 코드와 일회용 사이트를 이용한 개인별 네트워크인 DQ-Net의 연결 과정을 보여준다. AP는 공개키와 일회용 URL을 동적 QR 코드로 생성하여 디스플레이에 출력한다. 사용자는 자신의 기기로 이를 스캔하여 AP의 공개키를 얻게 되고, 자동적으로 일회성 페이지에 연결된다. 사용자가 일회성 페이지에서 요구하는 SSID와 암호를 입력하면, 이 정보들은 RSA 암호화 되어 public channel을 통해 AP로 전달된다. AP는 개인키를 이용하여 정보를 해독한 후 사용자에게 가상 Wi-Fi네트워크를 생성 제공하고, 이때 일회성 페이지는 자동 소멸한다.

2.1.1 일회성 페이지

DQ-Net은 일회성 페이지를 사용하여 SSID나 비밀번호와 같은 정보를 입력한다. 이 페이지에서 가장 중요한 점은 SSID 이름의 중복확인을 해준다는 점이다. 공유기의 초기 값을 변경하지 않거나, Fig. 3처럼 동일한 또는 가까운 채널에 같은 SSID의 Wi-Fi가 있다면 네트워크가 충돌해 느려지게 된다. 따라서 SSID 이름에 대한 중복확인은 네트워크의 느려지는 문제를 해결할 수 있다.

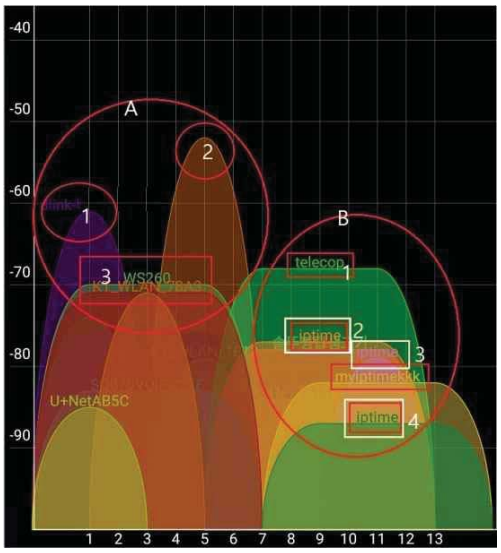

Fig. 3. For Wi-Fi with the same name of SSID on the same channel[4]

2.1.2 OTP (One Time Password)

OTP란 랜덤하게 만들어지는 난수를 일회용 비밀번호로 이용하는 것이다. 기존의 Wi-Fi는 보안성을 유지하기 위해 일정 기간마다 비밀번호를 변경해야 한다. 하지만 대부분의 사람들은 번거로움 때문에 변경하지 않는 경우가 많다. 이런 Wi-Fi를 공공장소에서 이용하면 시간이 지날수록 비밀번호를 아는 사람들의 숫자가 늘어나기 때문에 보안이 취약해진다. 그러므로 본 논문에서는 OTP 개념을 사용한다.

2.1.3 동적 QR 코드(Dynamic QR codes)

QR 코드는 누구나 자유롭게 생성할 수 있기 때문에 악성코드나 유해 웹사이트 주소도 전파가 가능하다. 이러한 악성 QR 코드는 사용자가 육안이

나 어플로 인지할 수 없기 때문에[6] 누군가 나쁜 의도를 가지고 QR 코드를 교체할 경우 큰 피해 상황이 발생할 가능성이 높다. 이것은 정적 QR 코드의 가장 취약한 점이며 많은 문제의 원인이 된다.

2.2 모드

DQ-Net은 장소에 따라 Wi-Fi 접속 방법을 달리하여 보안성을 유지할 수 있도록 하였다. 관리자 모드, 사용자 모드, 게스트 모드 세 가지로 나누었다.

2.2.1 관리자 모드 (Administrator Mode)

Fig. 4. Administrator Mode of DQ-Net
① Touch the Administrator Mode to the display
② Touch the Administrator Setting → Confirm the OTP number
③ Output dynamic QR codes to the display → Scan the QR codes with the Smart Phone → Link to disposable page
④ Enter the information(SSID, P/W) at the site → RSA Encryption → Convey information to AP via public channel
⑤ Decode the data with AP private key → Create and provide virtual Wi-Fi Networks

관리자 모드는 일반적인 네트워크 연결 과정과 상당히 유사하다. 관리자란, 네트워크를 설치한 이후 최초로 기기를 등록한 사람에게 부여되는 권한이다. 관리자는 OTP 카드를 갖게 되는데, 이 카드는 처음 기기 등록과 비밀번호 바꾸는 주기 변경, 사용자 권한 부여 작업에 사용된다. 처음 AP기기를 켠 후 관리자 모드를 선택한다. 이후에 뜨는 하위 메뉴에서 관리자 등록을 누르고 키패드가 뜨면, 이용자는 OTP 번호를 입력하여 자신이 관리자라는 것을 인증하다. 일회성 등록 사이트로 이동할 수 있는 QR 코드가 디스플레이에 표시되면 이용자는 스마트폰을 통해 QR 코드를 인식하여 일회성 페이지로 접속한다. SSID와 비밀번호 등 필요한 정보들을 입력하고 비밀번호가 자동으로 바뀌는 주기를 설정한다.

2.2.2 사용자 모드 (User Mode)

사용자 모드는 게스트 모드와 달리 지속적으로 네트워크를 이용할 수 있다. 사용자는 관리자와 동일한 네트워크를 사용하기 때문에 관리자로부터 권한을 부여받아야한다. 관리자의 가상 네트워크망을 공유하기 때문에, 별도의 네트워크 생성과정이 필요하지 않다.

Fig. 5. User Mode of DQ-Net
① Touch the Administrator Mode to the display
② Touch the User Setting → Output dynamic QR codes to the display → Scan the QR codes with the Smart Phone
③ Create and provide virtual Wi-Fi Networks

우선 사용자는 AP 기기의 디스플레이에서 관리자 모드를 선택하고, 하위 메뉴에서 사용자 등록을 택한다. 사용자 등록을 누르면 번호를 입력할 수 있는 터치 키패드가 나오는데, 이곳에 관리자의 OTP카드의 번호를 입력한다. 확인이 완료되면 관리자의 네트워크 정보가 담긴 QR 코드가 생성된다. 사용자의 기기로 이 QR 코드를 스캔하고 네트워크 접속을 묻는 알림에 확인을 누르면 네트워크 연결이 완료된다. 그 과정은 Fig.5와 같다.

2.2.3 게스트 모드 (Guest Mode)

게스트 모드는 가상 네트워크를 지속적으로 사용하지 않는 이용자를 위한 모드이다. 따라서 관리자 모드, 사용자 모드와는 달리 연결이 끊길 경우 자동적으로 가상 Wi-Fi 공간이 소멸된다. 다른 모드들과는 달리 게스트 모드는 가정용과 상업용으로 나뉘는데, 용도에 따라 사용방법 면에서 차이를 보인다.

가정용의 경우 AP의 디스플레이에서 게스트 모드를 터치하면 일회성 사이트로 이동할 수

있는 QR 코드가 생성된다. 게스트는 이 QR 코드를 스캔하여 일회성 사이트에 접속하고 SSID와 비밀번호를 설정한다. 페이지에서 확인을 누르면 가상 네트워크망이 생성되고 자동으로 게스트의 스마트폰에서 네트워크 연결이 된다.

상업용의 경우 AP기기와 연동이 되는 기계를 각 카운터에 두어 버튼을 누르면 QR 코드가 출력된 스티커가 나오게 할 수 있다. 이 부착물을 가상 네트워크를 사용하는 게스트의 영수증에 붙여 전달하고, 그 이후의 과정은 가정용에서의 과정과 일치한다.

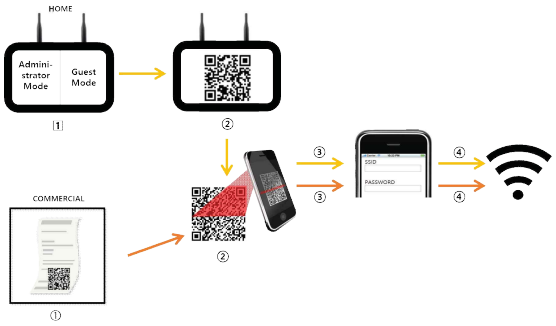

Fig. 6. Guest Mode of DQ-Net (For Home & Commercial Use)
⓵ Touch the Guest Mode to the display → Output dynamic QR codes to the display
① Attach QR codes sticker to receipt or product
② Scan the QR codes with the Smart Phone → Link to disposable page
③ Enter the information(SSID, P/W) at the site → RSA Encryption → Convey information to AP via public channel
④ Decode the data with AP private key → Create and provide virtual Wi-Fi Networks

2.3 성능평가

Table. 1. Improvement result

	As-Found	Suggestion
Security Performance	LOW	HIGH
Convenience	LOW	HIGH

본 논문에서는 동적 QR 코드를 사용함으로써 정적 QR 코드의 보안적 문제점 해결방안을 제시한다. 또한 사용자의 정보를 입력하는 과정에서 일회용 사이트를 이용하는 것은 애플리케이션의 설치를 필요로 하지 않아 사용이 간편하게 만들어준다. 모드를 분류하여 네트워크를 사용하는 것은 관리를 용이하게 한다. 관리자 모드를 통해 관리자에게만 OTP카드의 이용 및 관리 권한을 부여하는 것은 보안성을 높이는 방법이며, 이용시간이 길지 않은 공공장소 등에서의 게스트 모드 사용은 네트워크 이용을 편리하게 한다.

III. 결론

본 논문에서는 사용자 중심 네트워크를 제안한다. 사용자가 스스로 AP를 설정하여 Wi-Fi 네트워크를 이용한다. 이에 사용되는 Wi-Fi 환경은 보다 구체적이고 보안성이 향상된 방안들을 제시한다. 또한, Wi-Fi를 사용하는 사람들의 목적에 따라 모드를 나눠 보안성을 유지할 수 있는 방안을 고려했다. 모드는 총 세 가지로 나누어졌다.

향후 이 기술이 보편적으로 사용되게 된다면 애플리케이션 설치 없이 보안성이 유지된 상태로 Wi-Fi 네트워크를 이용할 수 있게 될 것이다.

[참고문헌]

[1] Nam-seh Lee, Ju-ho Lee, Choong-Kyo Jeong, "PS-Net : Personalized Secure Wi-Fi Network," *Journal of Korean Institute of Communications and Information Sciences*, 40(3) pp. 497-505, Mar. 2015.

[2] Hyung-Kyu Yang, "A study of Security Weaknesses of QR Codes and Its Countermeasures," *Journal of The Institute of Internet, Broadcasting and Communication*, 12(1), Feb. 2012.

[3] Jae-Kyung Park, "Globl Report - Invasion of Wi-Fi security and current status of security techniques", *Journal of Radio Spectrum & Communications*, June. 2010.

[4] SSID, https://bit.ly/2TERI1D

[5] "무료 와이파이 사용자 노트북 해킹당해...은행 잔고 털려," Daily Secu, Accessed: 2014-04-15.

[6] QR code, https://bit.ly/2r2nAA5, Accessed : 2011-05-24