http://dx.doi.org/10.14400/JDPM.2013.11.12.453

무선 LAN 연결 해제 공격과 보안

홍성혁*
백석대학교, 정보통신학부

Disconnection of Wireless LAN Attack and Countermeasure

Sunghyuck Hong*
Baekseok University, Division of Information and Communication

요 약 무선 LAN 환경에서는 최대한 안전한 것이 가장 중요하다. 표준 802.11 보안은 매우 네트워크 공격에 대해 매우 많은 취약점을 가지고 있다. IEEE 에서는 이러한 취약점에 대해서 보안을 하기 위해 많은 메커니즘을 만들지만, 무선 LAN의 특성인 공중에 브로드 캐스트 하는 방식 때문에 다른 환경의 네트워크 보다 많은 정보가 유출 될 수 있다. 무선 LAN 환경에서 해당 인증 이후에 무선 LAN에 접근 할 수 있기 때문에 이러한 인증 과정이 중요한 것이다. 하지만 인증 과정에는 안전적인 메커니즘이 사용하지만, 근본적인 최대한의 정보 노출을 줄이는 방법에 대해서는 언급하지 않고 있는 실태이다. 해당 연구에서는 무선 LAN의 인증과 인증 해제 방법과 이에 대한 취약점에 대해서 설명하고, 해당 취약점에 대한 보안 방법을 제시한다.

주제어 : 802.11 클라이언트 인증, 인증 해제 공격에 대한 대응, Connected Value 생성, Connected Value 인증

Abstract In a wireless LAN environment, security is the most important. Security of 802.11 standard has many vulnerabilities of the network attack. IEEE has created mechanisms to security for this vulnerability. But the vulnerabilities is characteristic of broadcast in the air in wireless LAN, it is more disclosure then other network environments. In a wireless LAN environment, it can be accessed to the wireless LAN after authentication. Authentication process is one of most important because of the first security step. However, in the authentication process is not mentioned in the method of reducing the disclosure maximum fundamental. Therefore, in this research, the vulnerability of 802.11 are presented and how to do de-authentication in 802.11.

Key Words : 802.11 client authentication, the authentication response to the attack, release, Connected Value creation, Connected Value authentication, MAC address and Connected Value

1. 서론

최근 무선 인터넷 단말기(랩탑, 스마트폰 등)의 급격한 보급으로 인해, 전국적으로 기업/가정에 무선 AP(Access Point)가 설치되고 있다. 이러한 무선 AP의 설치는 무선 인터넷 단말기를 사용하는 사용자는 편리하지만, 보다 쉽게 해당 네트워크에 접속할 수 있는 위험성을 가지고 있다. 그렇기 때문에 무선 AP에 접근하기 위해서는 많은 보안 프로토콜을 사용하고 있다. WEP, WPA나 WPA2와 같은 보안 프로토콜을 사용한다. 그러나 이러한 보안 프로토콜만으로는 안전한 무선 LAN을 구축하기는 어렵다. 많은 해커들과 해킹 도구들을 이용

* This research was partially supported by Baekseok University.
Received 15 October 2013, Revised 17 December 2013
Accepted 20 December 2013
Corresponding Author: Hong, Seong Hyuk(Baekseok University)
Email: shong@bu.ac.kr

ISSN: 1738-1916

해 위의 보안 프로토콜들을 공격하고 있고, 그로 인해 취약점들이 드러났다. 이보다 더 안전하게 무선 LAN을 사용하기 위해 무선 AP의 SSID를 숨기는 방법을 사용하지만, 이러한 방법 역시 공격당해 보안 능력을 잃어버렸다. 이 논문에서는 위 보안 프로토콜을 이용한 보안을 더욱 강화시키기 위한 방법을 제시한다.

2. 802.11 인증

IEEE 802.11은 흔히 무선랜, 와이파이(Wi-Fi)라고 부르는 무선 근거리 통신망(Local Area Network)을 위한 컴퓨터 무선 네트워크에 사용되는 기술로, IEEE의 LAN/MAN 표준 위원회 (IEEE 802)의 11번째 워킹 그룹에서 개발된 표준 기술을 의미한다. WEP(Wired Equivalent Privacy)키가 정확하지 않은 클라이언트는 무선 AP와 통신이 불가능하기 때문에 WEP키를 사용하면 액세스 컨트롤 하는 효과를 얻을 수 있다. [2]

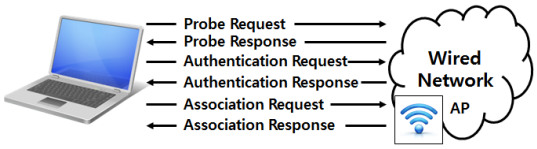
2.1 SSID(Service Set Identifier)

SSID는 무선 LAN을 논리적으로 분할할 수 있는 구조를 가지고 있다. 일반적으로 적절한 SSID로 클라이언트를 구성해야 무선 LAN에 액세스 할 수 있다. SSID는 데이터 프라이버시 기능을 제공 하지 않으며 실제로 클라이언트를 AP에 인증하지도 않는다.

2.2 802.11 스테이션 인증

802.11 사양에서 인증은 사용자 인증 대신 무선 장치를 인증하는 방식을 사용한다. 802.11 사양에서 개방형 인증과 공유키 인증 모드를 제공한다. fig. 1과 같이 802.11 클라이언트 인증 프로세스는 다음과 같은 트랜잭션으로 구성 한다.[3]

1. 클라이언트가 모든 채널에서 프로브 요청 프레임을 브로드캐스트 한다.
2. 범위 내에 있는 무선 AP가 프로브 응답 프레임을 통해 응답(reply)한다.
3. 클라이언트가 액세스에 가장 적합한 무선 AP를 선택한 후 인증 요청을 전송한다.
4. 무선 AP가 인증 응답을 전송한다.
5. 인증이 성공이후 클라이언트가 무선 AP에 연결 요청 프레임을 전송한다.
6. 무선 AP가 연결 응답을 한다.
7. 클라이언트가 무선 AP와 통신할 수 있게 된다.



[Fig. 1] 802.11 Client Authentication Processes

2.2.1 프로브 요청 및 응답

클라이언트가 활성화가 되면 프로브 요청 프레임을 사용하여 사용 가능한 무선 AP를 검색한다. Fig. 2와 같이 프로브 요청 프레임을 클라이언트가 사용 가능한 모든 채널로 전송하여 SSID와 클라이언트 요청 데이터 속도가 같은 사용가능한 모든 무선 AP를 찾아낸다.[2] 사용가능 하고 프로브 요청 기준에 적합한 모든 AP는 프로브 응답 프레임을 통해 응답한다. 프로브 응답 프레임에는 동기화 정보 및 액세스 포인트 로드를 포함해야 한다. 이러한 정보를 검토하여 어떤 AP에 연결 할 것인지 결정한다. 클라이언트에서 연결한 AP를 결정하면 802.11 네트워크 액세스 인증단계로 넘어간다.[4]

```
DLC: ----- DLC Header -----
DLC:
DLC: Frame 201 arrived at  10:18:59.4328; frame size is 39 (0027 hex) bytes.
DLC: Signal level                  = 100%
DLC: Channel                       = 1
DLC: Data rate                     = 2 ( 1.0 Megabits per second)
DLC:
DLC: Frame Control Field #1 = 40
DLC:                .... ..00 = 0x0 Protocol Version
DLC:                .... 00.. = 0x0 Management Frame
DLC:                0100 .... = 0x4 Probe request (Subtype)
DLC: Frame Control Field #2 = 00
DLC:                .... ...0 = Not to Distribution System
DLC:                .... ..0. = Not from Distribution System
DLC:                .... .0.. = Last fragment
DLC:                .... 0... = Not retry
DLC:                ...0 .... = Active Mode
DLC:                ..0. .... = No more data
DLC:                .0.. .... = Wired Equivalent Privacy is off
DLC:                0... .... = Not ordered
DLC: Duration                      = 0 (in microseconds)
DLC: Destination Address           = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source Address                = Station Airont500292
DLC: Basic Service Set ID          = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Sequence Control              = 0x6F30
DLC: ...Sequence Number            = 0x6F3 (1779)
DLC: ...Fragment Number            = 0x0   (0)
DLC: Element ID                    = 0 (Service Set Identifier)
DLC: ...Length                     = 7 octet(s)
DLC: ...Service Set Identity       = "sliders"
DLC:
DLC: Element ID                    = 1 (Supported Rates)
DLC: ...Length                     = 4 octet(s)
DLC: ...Supported Rates information field = 02
DLC:                               0... .... = Not Basic Service Set Basic Rate
DLC:                               .000 0010 =  1.0 Megabits per second
DLC: ...Supported Rates information field = 04
DLC:                               0... .... = Not Basic Service Set Basic Rate
DLC:                               .000 0100 =  2.0 Megabits per second
DLC: ...Supported Rates information field = 0B
DLC:                               0... .... = Not Basic Service Set Basic Rate
DLC:                               .000 1011 =  5.5 Megabits per second
DLC: ...Supported Rates information field = 16
DLC:                               0... .... = Not Basic Service Set Basic Rate
DLC:                               .001 0110 = 11.0 Megabits per second
```

[Fig. 2] Request Prob Frame

2.2.2 개방형 인증

개방형 인증은 Null 인증 알고리즘을 사용한다. AP는 모든 인증 요청에 대해 승인한다. 1997 802.11 사양에서의 인증은 중점은 연결에 맞춰져있다.[5] 인증을 하기위한 요구사항은 보안적인 측면이 아닌 신속하게 무선 AP와 통신을 할 수 있게 하는 것 이다

개방형 인증은 다음과 같이 개방형 인증 요청 Fig. 3과 개방형 인증 응답 Fig. 4로 구성되어 있다.[3]

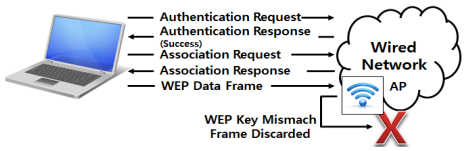
```
DLC: ----- DLC Header -----
DLC:
DLC: Frame 95 arrived at  10:49:47.8255; frame size is 30 (001E hex) bytes.
DLC: Signal level                = 100%
DLC: Channel                     = 1
DLC: Data rate                   = 2 ( 1.0 Megabits per second)
DLC:
DLC: Frame Control Field #1 = B0
DLC:               .... ..00 = 0x0 Protocol Version
DLC:               .... 00.. = 0x0 Management Frame
DLC:               1011 .... = 0xB Authentication (Subtype)
DLC: Frame Control Field #2 = 00
DLC:               .... ...0 = Not to Distribution System
DLC:               .... ..0. = Not from Distribution System
DLC:               .... .0.. = Last fragment
DLC:               .... 0... = Not retry
DLC:               ...0 .... = Active Mode
DLC:               ..0. .... = No more data
DLC:               .0.. .... = Wired Equivalent Privacy is off
DLC:               0... .... = Not ordered
DLC: Duration                    = 314 (in microseconds)
DLC: Destination Address         = Station Airont31669C
DLC: Source Address              = Station Airont500292
DLC: Basic Service Set ID        = Airont31669C
DLC: Sequence Control            = 0x0A40
DLC: ...Sequence Number          = 0x0A4 (164)
DLC: ...Fragment Number          = 0x0   (0)
DLC: Authentication algorithm number = 0 (Open System)
DLC: Authentication transaction sequence number = 1
DLC: Status code                 = 0 (Reserved)
```

[Fig. 3] Open Authentication Request Frame

```
DLC: ----- DLC Header -----
DLC:
DLC: Frame 97 arrived at  10:49:47.8279; frame size is 30 (001E hex) bytes.
DLC: Signal level                = 81 %
DLC: Channel                     = 1
DLC: Data rate                   = 22 (11.0 Megabits per second)
DLC:
DLC: Frame Control Field #1 = B0
DLC:               .... ..00 = 0x0 Protocol Version
DLC:               .... 00.. = 0x0 Management Frame
DLC:               1011 .... = 0xB Authentication (Subtype)
DLC: Frame Control Field #2 = 00
DLC:               .... ...0 = Not to Distribution System
DLC:               .... ..0. = Not from Distribution System
DLC:               .... .0.. = Last fragment
DLC:               .... 0... = Not retry
DLC:               ...0 .... = Active Mode
DLC:               ..0. .... = No more data
DLC:               .0.. .... = Wired Equivalent Privacy is off
DLC:               0... .... = Not ordered
DLC: Duration                    = 258 (in microseconds)
DLC: Destination Address         = Station Airont500292
DLC: Source Address              = Station Airont31669C
DLC: Basic Service Set ID        = Airont31669C
DLC: Sequence Control            = 0xED50
DLC: ...Sequence Number          = 0xED5 (3797)
DLC: ...Fragment Number          = 0x0   (0)
DLC: Authentication algorithm number = 0 (Open System)
DLC: Authentication transaction sequence number = 2
DLC: Status code                 = 0 (Successful)
```

[Fig. 4] Open Authentication Response Frame

개방형 인증은 연결하고자 하는 모든 클라이언트는 네트워크 액세스를 얻을 수 있다. 네트워크상에서 암호화가 이루어지지 않는 경우 무선 AP의 SSID를 알고 있는 장치가 네트워크 액세스 컨트롤 하는 권한을 가진다. 무선 AP에서 WEP 암호화가 이루어지는 경우 WEP 키가 액세스 컨트롤을 하게 된다. Fig. 5와 같이 클라이언트가 올바른 WEP키를 가지고 있지 않다면 인증에 성공하더라도 무선 AP를 통해 통신할 수 없다. 또한 무선 AP에서 전송받은 데이터를 복호화 할 수 없다.[3]



[Fig. 5] Each different WEP key in Open Authentication

2.2.3 공유 키 인증

공유 키 인증을 위해 클라이언트는 정적인 WEP키를 구성해야 한다. 공유키 인증은 Fig. 6와 같은 과정을 통해 통신한다.[3]

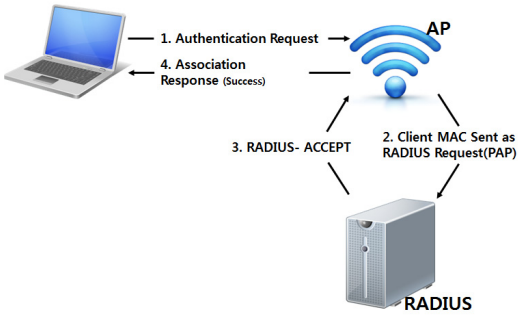
1. 클라이언트가 로컬로 구성된 WEP키를 이용하여 해당 텍스트를 암호화 하고 후속 인증 요청을 전송한다.
2. 무선 AP 가 인증 요청을 복호화 하고 원래의 텍스트를 확인 할 수 있는 경우, 무선 AP는 클라이언트에 액세스를 승인하는 인증 응답을 전송한다.
3. 클라이언트가 로컬로 구성된 WEP키를 이용하여 해당 텍스트를 암호화 하고 후속 인증 요청을 전송한다.
4. 무선 AP 가 인증 요청을 복호화 하고 원래의 텍스트를 확인 할 수 있는 경우, 무선 AP는 클라이언트에 액세스를 승인하는 인증 응답을 전송한다.

[Fig. 6] Shared Key Authentication Process

2.2.4 MAC 주소 인증

MAC 주소 인증은 표준화 되지 않은 메커니즘이지만

많은 무선 AP제조사에서 지원하는 방식이다. MAC 주소 인증은 클라이언트의 MAC 주소가 LAN으로 연결된 허용 주소 목록 또는 외부 인증 서버에 있는 MAC 주소에 저장되어 있다면 통신이 되는 방식이다.[6]



[Fig. 7] MAC Address Authentication Process

2.2.5 Hidden SSID

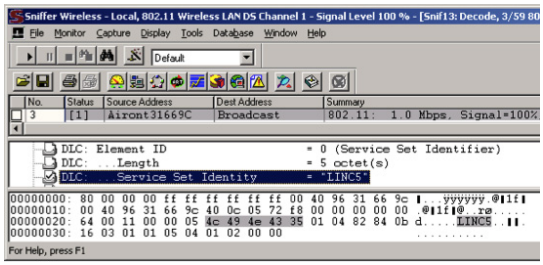
Hidden SSID란 무선 AP에서 신호를 브로드캐스트(Broadcast)할 때 자신의 SSID를 지우고 송출하는 방법을 사용하는 기법이다. 따라서 해당 무선 AP에 연결하고자 하는 장치(PC, 랩탑, 스마트폰 등)에서 은폐된 SSID를 직접 입력하여 해당 무선 AP의 SSID가 일치하면 연결이 되는 방법이다. 이 기술을 사용하면 해커가 무선 AP에 접근하려 할 때 무선 AP의 SSID를 알 수 없기 때문에 즉시 공격이 어려워진다.

그러나 SSID는 보안요소가 포함되어 있는 것이 아니기 때문에 SSID를 은폐시킬 경우 WI-FI 운영상 악영향을 미칠 수도 있다.[6]

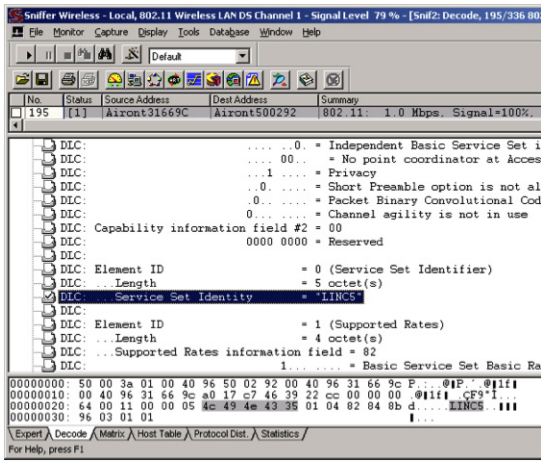
2.3 인증의 취약점

2.3.1 프로브 요청 및 응답

SSID는 무선 AP 비콘(Beacon) 메시지에서 (fig. 8)과 같이 암호화 되지 않은 상태로 공개된다. 사용자가 비콘 메시지를 볼 수 있지만, 해커들은 무선 LAN 패킷 분석 도구와 같은 해킹 도구를 사용하여 SSID를 쉽게 확인 할 수 있다.[7] 무선 AP 제조업체에서는 비콘 메시지에서 SSID를 브로드캐스트 하지 않도록 지원하지만, 해커들은 여러 방법을 통해 SSID를 확 할 수 있다. Fig. 9과 같이 Hidden SSID 환경에서도 프로브 응답 프레임을 이용하여 SSID를 확인 할 수 있다.[3]



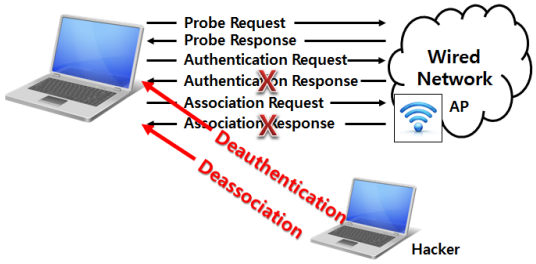
[Fig. 8] Wireless AP Become Frame's SSID



[Fig. 9] Wireless AP Prob Response Frame's SSID

2.2.2 De-authentication 공격

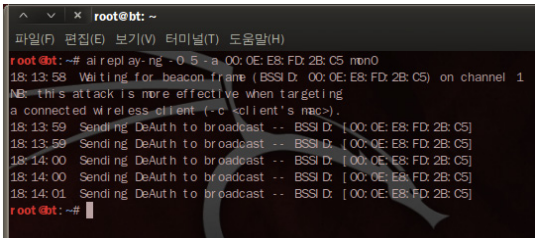
이 공격은 특정 AP에 연결되어 있는 클라이언트들을 연결 해제 시키는 패킷을 보내어, 해당 AP에 연결된 모든 클라이언트가 연결 해제 된다.



[Fig. 10] De-authentication Attack Process

해커는 AP와 연결되어 있는 클라이언트의 MAC 주소를 스니핑하여 해당 클라이언트의 MAC주소로 AP에게 인증 해제 패킷을 전송한다. 무선 AP는 인증 해제 패킷을 받고 클라이언트와 연결을 해제 한다.[7]

Fig. 11은 리눅스의 일종인 Backtrack 5에서 Aireplay 도구를 이용하여 De-authentication 공격하는 것을 캡쳐한 화면이다.



[Fig. 11] De-authentication attack in Blackberry

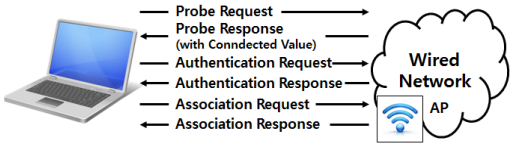
De-authentication 공격 이후 연결 해제된 클라이언트는 무선 AP와 재접속을 요청할 때 숨겨진 SSID, 인증에 필요한 키 값과 같은 정보들을 다시 전송하게 된다.

3. 제안하는 인증 및 연결 해제 과정의 보안

인증 과정 이후 외부에서 접근하고자 하는 공격자들에게 정보를 유출을 최소화하기 위해서는, 공격 이전에 연결되어 있던 상태를 유지하는 것이 중요하다. 연결이 강제로 해제되면 재 인증을 위해 인증 과정이 다시 성립하게 되고, 그 과정에서 공격자들은 정보를 획득하거나 접근할 수 있는 여지를 가지게 된다. 따라서 최초 인증 시 지속적인 연결을 위해 다음과 같은 과정이 추가 되는 것을 제시 한다.

3.1 고유한 Connected Value 생성

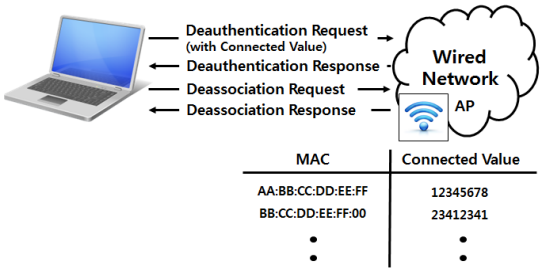
클라이언트에서 무선 AP로 연결을 요청할 때 무선 AP는 고유한 Connected Value값을 생성하여 클라이언트에게 전송한다. 이 값은 연결이 해제되기 전까지 클라이언트와 무선 AP는 저장한다.



[Fig. 12] Connected Value added in 802.11 Client Authentication Process

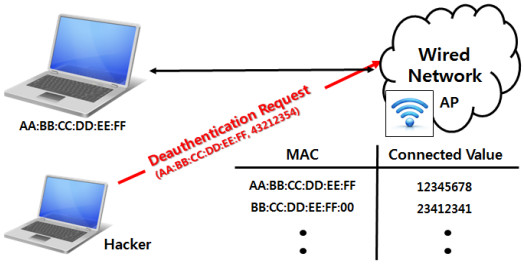
3.2 연결 해제 요청 시 Connected Value 인증

클라이언트에서 연결 해제 요청 시 무선 AP에 연결 인증 시 전송받은 Connected Value를 함께 전송한다. 연결 해제 요청 프레임과 Connected Value를 전송 받은 무선 AP는 무선 AP에 저장되어 있는 MAC 주소와 Connected Value를 함께 대조하여 일치하는 값이 있다면 해당 MAC 주소에 대한 연결에 대해 De-authentication 한다. 만약 MAC 주소와 Connected Value 가 일치하는 값이 없다면, 기존의 연결된 상태로 유지된다.



[Fig. 13] Secured De-authentication Process

위 그림과 같이 AP는 인증이 성립된 클라이언트의 MAC 주소와 해당 MAC 주소에 대응하는 Connected Value 값이 일치하게 되면 정상적으로 연결이 해제되는 단계를 이룬다.



[Fig. 14] Secured 802.11 Client Authentication Process in De-authentication Attack Situation

보안된 802.11 클라이언트 인증 프로세스에서는 위 그림과 같이 해커가 De-authentication 공격 하더라도 해당 MAC 주소와 MAC 주소에 대응하는 Connected Value 값이 일치 하지 않기 때문에 해커의 의도대로 연결이 해제되지 않는다.

4. 결론

802.11 클라이언트 인증에는 강제 연결 해제 시 인증 회피에 대한 취약한 점을 가지고 있다. IEEE에서는 802.1X를 통해 더욱 강력한 인증을 제공함으로 무선 LAN 환경을 더욱 안전성을 보장한다. 그러나 이러한 인증은 세션 하이재킹 공격에 의해 공격자에 의해 쉽게 인증 해제 되고, 클라이언트는 다시 인증하기 위해 암호화 되지 않은 프레임을 브로드캐스트 하게 된다. 따라서 본 연구에서는 인증 해지 시 기존에 연결된 인증 방식을 고수함으로써 연결해제를 통한 세션 하이재킹을 막을 수 있어, 인증 해제에 대한 취약점을 보안할 수 있다. 인증이 강제로 해제가 되던지 아니면 네트워크 불량으로 접속이 끊어지면 즉시 초기의 인증을 요청하는 프로세스를 실행시켜(connected value 교환) 세션하이재킹을 막으면 강제 해제로 인한 인증 회피를 막을 수 있다.

REFERENCES

[1] doi: 10.1109/IEEESTD.2005.97890

[2] Lashkari, A.H.; Danesh, M.M.S.; Samadi, B., "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," Computer Science and Information Technology, 2009.

[3] Baghaei, N.; Hunt, R., "IEEE 802.11 wireless LAN security performance using multiple clients," Networks, 2004. (ICON 2004). vol.1, no., pp. 299-303 2004

[4] doi: 10.1109/IEEESTD.2010.5605400

[5] Todd, H., "Secure applications – Hack-proofing your app," Electro/Information Technology (EIT), 2010 IEEE International Conference on, vol. 3, no. 1, pp. 20-22, 2010

[6] Fang Lan; Wang Chunlei; Ma Guoqing, "A framework for network security situation awareness based on knowledge discovery," Computer Engineering and Technology (ICCET), 2010 2nd International Conference on , vol.1, no., pp.226-231, 2010

[7] Vivek Ramachandran, BackTrack 5 Wireless Penetration Testing, Vol. 2 pp 66-70, 2013.

[8] Zhihu Wang, "Design and realization of computer network security perception control system," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp. 27-29, 2011

[9] Bensaou, B.; Zuyuan Fang, "A Fair MAC Protocol for IEEE 802.11-Based Ad Hoc Networks: Design and Implementation," Wireless Communications, IEEE Transactions on, vol.6, no.8, pp. 2934-2941, 2007

[10] Li Wang; Srinivasan, B., "Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard," Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on , vol.2, no., pp. 109-113, 2010

[11] Elgraini, M.T.; Assem, N.; Rachidi, T., "Host intrusion detection for long stealthy system call sequences," Information Science and Technology (CIST), 2012 Colloquium in , vol., no., pp. 96-100, 2012

홍 성 혁(Hong, Sung Hyuck)

- 1995년 2월 : 명지대학교 컴퓨터공학과 (공학사)
- 2007년 8월 : Texas Tech University, Computer Science(공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 네트워코 보안, 해킹, 센서 네트워크 보안
- E-Mail : shong@bu.ac.kr