https://doi.org/10.7840/kics.2022.47.11.1788

STRIDE 위협 모델링을 이용한 무선 네트워크 공유기 위협 분석

강 수 진◆°, 조 현 석*, 신 영 섭*, 조 규 태*

Threat Analysis of the Wireless Network Router Using STRIDE Threat Modeling

Su-jin Kang◆°, Hyun-suk Cho*, Young-seop Shin*, Kyu-tae Cho*

요 약

무선 네트워크만의 장점과 편리함에 힘입어 무선망의 사용량은 급격히 증가하고 있으며, 개인뿐만 아니라 공공기관, 기업에서도 필수 서비스로 무선 Wi-Fi 서비스를 제공하고 있다. 그에 따라 무선 네트워크 공유기를 대상으로 하는 공격 역시 해마다 증가하고 있으며 취약점이 발생하여 개인의 중요 정보 유출, 서비스 중단 등이 발생할 경우 막대한 피해가 발생하고 있다. 무선 공유기는 확보 및 접근성이 용이하지만, 유선 네트워크와 달리 물리적인 접근 없이도 공격이 발생할 수 있고, 무선 공유기 제품마다 제공하는 보안프로토콜 등 그 수준이 상이하여 무선 공유기에 대한 위협 분석을 통한 취약점 분석이 중요하다. 본 논문에서는 무선 네트워크 공유기의 데이터 흐름도(DFD)를 작성하여 네트워크 공유기와 인터넷 기기 사이에 데이터 흐름을 분석하고, STRIDE 위협 모델링 기법을 적용하여 위협을 체계적으로 식별하였다. 또한, 공격 트리를 작성한 뒤 공격 시나리오를 도출하여 DREAD를 적용한 위험도 분석을 수행하였다. 최종적으로 이러한 위협 모델링의 결과를 기반으로 무선 네트워크 공유기의 보안 기능을 점검하기 위한 체크리스트를 제안하여 무선 네트워크 공유기의 보안성 향상에 기여하고자 한다.

Key Words : Threat Modeling, Risk Analysis, STRIDE, Network Router

ABSTRACT

Due to the advantages and convenience of wireless networks, the use of wireless networks is rapidly increasing, and not only individuals, but also public institutions and businesses are providing wireless Wi-Fi services as essential services. As a result, attacks targeting wireless network routers are also increasing every year, and when vulnerabilities occur, enormous damage occurs. Because Wireless routers are easy to secure and access, attacks can occur without physical access. And the level of security protocols provided by wireless router products is different, so it is important to analyze vulnerabilities through threat analysis on wireless routers. In this paper, we created a data flow diagram (DFD) of a wireless network router, analyzed the data flow between the network router and Internet devices, and applied the STRIDE threat modeling technique to systematically identify threats. Additionally we applied the attack tree, and DREAD model to threats. Finally, a checklist for checking the security functions of the wireless network router is proposed to contribute to the improvement of the security of the wireless network router.

◆° First and Corresponding Author : LIG Nex1 Co., pulip0323@naver.com, 정회원
* LIG Nex1 Co., ambitihyun@naver.com; busigee@naver.com; kyutae.cho@gamil.com
논문번호 : 202206-121-B-RN, Received June 22, 2022; Revised August 12, 2022; Accepted August 22, 2022

Ⅰ. 서 론

유선 랜이 제공할 수 없는 무선 랜만의 다양한 장점과 편리함에 힘입어 현대 사회에서 무선 네트워크 공유기를 활용한 무선 랜 환경은 필수가 되었다. 가정에서는 PC 이외에 개인용 모바일 기기, 스마트 가전 기기의 보급이 확대되었고, 카페 등 대다수의 상업시설에도 공용 Wi-Fi를 필수 서비스로 제공하고 있다. 그 용도 또한 단순한 인터넷 서핑이 아닌 개인 신분정보 열람/변경, 인터넷 뱅킹 등 그 중요도가 올라가고 있다. 하지만 보안에 취약한 무선 공유기가 급증함에 따라서 이에 대한 보안 공격의 위험성 또한 늘고 있다.

2017년 Norton 사에서 공용 Wi-Fi에 대한 소비자 인식을 조사한 리포트[1]에 따르면 세계 소비자의 55%가 무료 Wi-Fi 사용을 위해서는 안전하지 않은 무선 랜에 대한 접속을 허용한다. 또한, 보안 위험이 있더라도 개인 이메일, 금융 정보 접속 등의 활동에서 보안 위험을 감수할 수 있다고 87%가 답하였다. 이를 통해 일부 무선 랜 사용자는 이를 위험하다고 인식하면서도 사용을 유지하고 더불어 공용 Wi-Fi에 연결할 때 위험을 인식하지 못하고 계속해서 개인정보를 위험에 빠뜨리기도 한다.

무선 네트워크 공유기 보안 사고로 인한 피해는 매우 다양하다. 유사한 가짜 웹 페이지를 만들어 접속하게 한 뒤 개인정보를 훔치는 파밍(Pharming) 공격이나 공유기에 접속된 모든 인터넷 장치의 패킷을 스니핑(Sniffing)하여 금융정보 포털 사이트의 ID와 비밀번호와 같은 중요 정보를 훔칠 수도 있다. 특히 보안이 허술한 무선 공유기의 경우에는 다양한 해킹 사례[2]가 발생하면서 무선 네트워크 공유기의 보안 기능은 중요한 요소로 인식되고 있으나 공유기 제조업체마다 보안 기술 수준과 그 기준이 상이하여 체계적인 무선 네트워크 공유기에 대한 위협 분석과 관련된 연구의 필요성이 증가하고 있다.

따라서 본 논문에서는 무선 네트워크 공유기가 기본적으로 갖추어야 할 보안 기능을 분석하기 위해 위협 모델링(Threat Modeling)을 적용해 위협을 식별 및 분석하고, 이를 점검하기 위한 체크리스트를 도출한다.

본 논문 2장에서는 무선 네트워크 보안 프로토콜 및 관련 보안성 연구, 위협 모델링에 대한 관련 연구를 설명한다. 3장에서는 무선 네트워크 공유기에 위협 분석 모델링 절차를 적용하여 데이터 흐름도를 도출하고, 위협 분석을 수행한다. 이를 기반으로 Attack Tree를 작성하여 발생할 수 있는 공격 시나리오를 도출하고 DREAD 모델을 적용한 분석 결과를 제시한다. 4장에서는 무선 네트워크 공유기 보안성 평가를 위한 체크리스트를 도출하고 5장에서는 본 논문의 결론을 서술한다.

Ⅱ. 관련 연구

2.1 무선 네트워크 보안 프로토콜

무선 네트워크 공유기는 사용자가 인터넷에 로컬 네트워크를 무선으로 연결하기 위한 하드웨어 장치로 무선 통신 표준인 IEEE 802.11에 기반한 데이터 전송 규약인 Wi-Fi를 지원한다. 무선 네트워크 공유기의 보안과 관련된 주요 사양은 해당 공유기가 지원하는 무선 네트워크 보안 프로토콜에 따라 나누어진다.

WEP(Wired Equivalent Privacy)는 초기 무선 네트워크 암호화 통신 규약이다. 사전에 지정된 복호화 키를 AP(Access Point)와 단말기 사이에 공유하고, RC4(Rivest Cipher 4) 알고리즘을 통해 데이터를 암호화 해 전송하는 방식이다. 단, RC4 알고리즘 자체가 보안에 취약하며, 고정 암호키를 사용하기 때문에 암호화된 내용에 대해 공격자가 쉽게 해석할 수 있어 현재는 거의 사용되지 않는다.

WPA(Wi-Fi Protected Access)는 기존 WEP의 취약성에 대한 대안으로 기존의 고정키 대신, 동적 암호키 구현을 위해 TKIP (Temporal Key Integrity Protocol)를 적용한 기술이다. TKIP는 패킷당 키 할당, 키 값 재설정 등의 방식으로 암호키를 변경할 수 있다. 하지만 이 방식 역시 보안에 취약한 TKIP/RC4 알고리즘을 사용하기 때문에 안전한 기술은 아니다.[3]

무선 네트워크 보안 표준인 IEEE802.11i 규격이 2004년에 등장하면서, 이 규격에 맞춘 보안기술인 WPA2 프로토콜이 발표되었다. 고급 암호화 표준(AES) 기반 128bit 암호키를 사용하고, CCMP(CTR with CBC-NAC Protocol)를 통해 암호화하면서 기밀성과 무결성을 높였다. 하지만, 가장 안전한 보안 프로토콜로 평가되던 WPA2도 2017년 10월 KRACK[4]이라고 불리는 보안 취약점이 발견되었다. KRACK 취약점은 AP와 인터넷 장치가 서로 암호화 검증 메시지를 보내는 과정에서 해당 검증 메시지를 공격자가 탈취한 뒤 동일하게 전달해 오류를 일으키고, 암호키를 초기화하여 탈취한 데이터를 재조합하는 방식으로 공격이 이뤄진다.

2018년 이러한 문제를 해결하기 위해 WPA3 보안 프로토콜이 등장하였다. WPA3는 비밀번호 기반 보안 모드로 WPA3-SAE(Simultaneous Authentication of

Equals)를 사용하며 인증 단계에 Dragonfly 프로토콜을 적용하였다.[5] 그 중 WPA3-Personal은 WPA2와 동일한 암호화 알고리즘과 키 길이를 지원하고, WPA3-Enterprise는 암호화 무결성 알고리즘으로 GCMP (Galois/Counter Mode Protocol)를 도입하고 최소 192bit의 키를 사용하여 강화된 암호화를 제공한다.

그러나 WPA3 프로토콜도 완전히 안전하다고 보장할 수 없으며 WPA2에 지원하지 않았던 프로토콜을 도입하였기에 새로운 취약점들이 발생할 수 있다. WPA3를 지원하는 공유기가 출시되고 있지만 무선 네트워크 공유기 뿐만 아니라 이를 이용하는 클라이언트 제품들 역시 최신의 네트워크 프로토콜을 지원해야만 무선 랜을 사용할 수 있기 때문에 무선 공유기의 보안을 위해 무조건 최신의 무선 네트워크 프로토콜을 적용하기는 어렵다. 불특정 다수가 이용하는 공간에 구세대 보안 프로토콜이 적용된 무선 공유기가 있다면 이는 당연히 공격 대상이 될 수밖에 없다. 그러므로 위협 모델링을 통해 위협 분석을 진행하고 무선 공유기의 보안기능을 점검할 수 있는 체크리스트를 체계적으로 도출해야 한다. 또한, 무선 공유기 제공업체는 무선 공유기를 보다 안전하고 신뢰할 수 있도록 만들기 위해 식별된 보안 기능을 시스템에 반영하고 체계적으로 이를 점검해야 한다.

2.2 무선 네트워크 보안 연구 동향

무선 네트워크에 대한 보안 인식은 무선 랜이 도입된 초기부터 연구되었다.

Yulong Zou 외 3명은 무선 서비스의 신뢰성, 기밀성, 무결성 및 가용성 등 무선 네트워크의 보안 요구사항을 제시하고, 서로 다른 프로토콜 계층에서 무선 네트워크의 보안 취약성과 약점을 분석하였다. 또한, Wi-Fi 뿐만 아니라 블루투스, LTE 등 기존 무선 네트워크에서 사용되는 보안 프로토콜과 알고리즘을 정리하고, 무선 네트워크 혼합 공격, 크로스 레이어 무선 보안 설계 등 도전적인 무선 보안 과제들에 대해 제안하였다.[6]

Md. Waliullah와 Diane Gan은 IEEE 802.11 보안 표준과 관련된 취약점 및 보안 문제를 분석하여 기밀성/무결성/가용성 및 액세스 제어, 인증을 기반으로 한 공격/위협으로 분류하고 일반적으로 알려진 취약점과 위협을 방지하기 위한 가이드를 제시하고 있다.[7]

Aarthy Devi A. 외 2명은 특정 조직 환경 중 교육기관에 대해 라우터 네트워크 공격, WPA2 응답 공격 등과 같은 다양한 종류의 공격 시나리오를 만들어 네트워크 침투 실험을 수행하고 이러한 공격을 피하기 위한 네트워크 보안 위협 완화 전략을 제시하였다.[8]

위와 같이 무선 네트워크 보안과 관련된 여러 분야의 연구가 이루어지고 있지만 개발단계 초기인 설계 단계에서 체계적인 방법론을 적용하여 위협 및 공격 시나리오를 도출한 사례는 없다. 그러므로 위협 모델링을 통해 위협 분석을 진행하여 안전한 무선 네트워크 환경을 구축하기 위해서 무선 공유기가 반드시 갖추어야 하는 최소한의 보안 기능들을 정리하고자 한다. 본 논문에서는 무선 공유기 보안 기능에 중점을

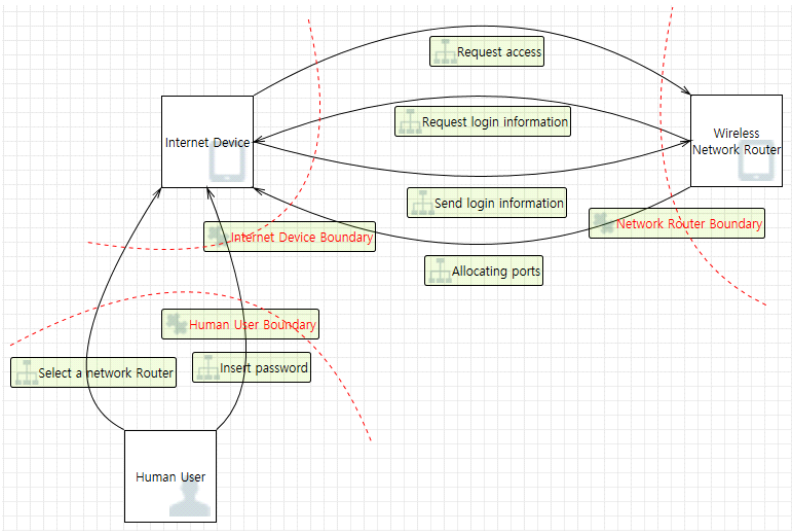


그림 1. 무선랜 공유기 Level 0 데이터흐름도
Fig. 1. Wireless Network Router Level 0 DFD

두고 Microsoft 위협 모델링 기법[9]과 도구[10]를 활용하여 발생할 수 있는 위협을 분석하였다.

2.3 위협모델링 연구 동향

위협 모델링은 분석 대상을 모델로 추상화한 뒤 체계적인 방법론을 통해 발생 가능한 위협을 식별하고 위험 분석을 통해 우선순위를 결정하여 이를 완화하기 위한 방법을 도출하는 보안성 분석 기술이다.[11]

현재 가장 많이 사용되는 모델은 1999년 Microsoft 사 내부에서 개발한 STRIDE[12] 모델이며 그 외에는 LINDDUN[13], PASTA[14], Trike[15] 모델 등이 있다.

STRIDE 모델[16]은 시스템 설계 과정에서 DFD (Data Flow Diagram)를 작성하고 데이터 흐름을 중심으로 위협을 분석한다. 위협은 위장(Spoofing), 변조(Tampering), 부인(Repudiation), 정보유출(Information disclosure), 서비스 거부(Denial of service), 권한 상승(Elevation of privilege)인 6가지 유형으로 분석한다. 또한, STRIDE 모델은 개발단계 초기인 설계 단계에서 위협을 체계적으로 분석할 수 있고 현재 가장 성숙된 기법으로 알려져 있다.[17]

STRIDE 모델을 활용한 위협모델링 연구는 데이터의 흐름과 노출 위협이 증가함에 따라 다양한 시스템 및 제품을 대상으로 진행되고 있다.

Markus Tasch, Rahamatullah Khondoker 외 2명은 SDN(Software Defined Networking)의 보안 응용 프로그램인 OpenFlow-Random Host Mutation과 Resonance을 STRIDE를 사용하여 분석하고 SDN 보안 응용 프로그램을 설계할 때 고려해야 할 사항을 도출하였다. 분석 시 DFD를 이용하여 시스템을 나타내었고 STRIDE를 통해 위협을 분석하였다. 특히 STRIDE와 유사한 위협 모델링 프레임워크인 Trike 등을 소개하며 그 중 STRIDE 분석을 사용한 이유에 대해 구체화 하고 있다.[18]

Anthony Hadding는 위협모델링을 이용하여 임베디드 시스템을 분석하였다. 시스템을 분석하기 위해 DFD를 이용하였고 위협 분석을 위해 Attack Tree를 사용하였다. 그리고 추가적으로 Microsoft Threat Modeling Tool과 Trike Threat Modeling Tool을 사용하여 분석을 진행하였다.[19]

Eun-ju Park 외 1명은 스마트팩토리의 전반적인 생산 공정 절차를 대상으로 DFD와 STRIDE 위협 모델링 기법을 적용하여 위협을 식별하는 연구를 수행하였다. 사이버 물리 시스템인 CPS(Cyber-Physical Systems)가 도입된 스마트팩토리에 STRIDE 모델을 적용하여 복잡도가 높은 시스템에 위협 식별을 체계적으로 진행하였다.[20] 그 외 AI 스피커[21], 스마트 홈 보안[22] 등 스마트 기기들에 대한 위협 모델링에 STRIDE 모델이 활용되고 있다.

본 논문에서는 무선 공유기를 시스템으로 분류하고 네트워크 통신에 대한 위협을 분석하는데 STRIDE 모델이 가장 적합한 것으로 판단하여 위협모델링 방법으로 Microsoft 사의 STRIDE 모델을 활용하였다.

Ⅲ. 네트워크 공유기 보안 위협 모델링

네트워크 공유기 보안 위협 모델링은 취약점 분석을 위한 범위 설정과 DFD 작성, 위협 식별 및 분석, Attack Tree 및 시나리오 작성, DREAD를 이용한 위험도 분석 순으로 수행하였다. 다음의 각 절에서 각 단계별 수행 결과를 설명한다.

3.1 분석 범위 및 제약사항 식별

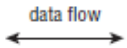
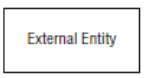
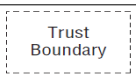
위협 모델링 전 네트워크 공유기의 분석 범위와 제약사항을 아래와 같이 설정해 두고 진행하였다.

1) 네트워크 공유기 로그인 시 PW, 소속 등 시스템별 다양한 정보를 요구하지만 로그인 시 필요 정보는 PW로 한정한다.
2) 스마트폰, 스마트 TV, 태블릿 PC, Lab-Top 등 네트워크 공유기를 이용할 수 있는 모든 기기는 이하 인터넷 기기로 한정 짓는다.
3) 사용자는 기존 네트워크 공유기에 권한을 얻은 사용자와 처음 네트워크 공유기에 접근하는 사용자, 네트워크 공유기를 관리할 수 있는 관리자로 나뉠 수 있지만 여기서는 최초 네트워크 공유기에 접근하여 권한을 얻는 사용자만 취급한다.
4) 위협 모델링 범위는 네트워크 공유기 접근 요청부터 네트워크 포트가 생성되는 과정까지 한정 짓는다.
5) 네트워크 공유기에 실제 IP, DNS를 제공하는 서버는 생략한다.

3.2 DFD(Data Flow Diagram)를 통한 데이터 흐름 분석

DFD는 데이터의 흐름에 따라 시스템의 구조와 동작을 모델링 및 도식화하기 위해 작성하는 그림으로 Microsoft STRIDE 위협 모델링의 기본 입력이 된다.[23] 따라서 본 논문에서도 DFD를 통해 네트워크 공유기에 대한 동작을 분석한다.

표 1. DFD 구성
Table 1. DFD elements

Element	Appearance	Meaning
Process		Any running code
Data Flow		Communication between processes, or between processes and data stores
Data store		Things that store data
External entity		People, or code outside your control
Trust Boundary		Changes of privilege levels

DFD의 구성 요소는 표 1과 같다. DFD 레벨 0은 외부 엔터티 간 또는 외부 엔터티와 관계가 있는 단일 프로세스로 시스템을 보여주는 추상화 단계로 컨텍스트 다이어그램이라고도 부른다. 그림 1은 레벨 0의 DFD로써 네트워크 공유기와 인터넷 기기에서 각각의 프로세스를 수행하며, 3.1절에서 제시한 분석 범위에 따라 사용자가 네트워크 공유기를 선택하고, 로그인에 성공해 포트가 할당되는 범위까지 한정하여 데이터 흐름을 나타냈다.

레벨 1의 DFD는 레벨 0보다 추상화 정도가 낮으며 여러 프로세스로 분해된다. 이 레벨에서는 시스템의 주요 기능을 강조하고 레벨 0 수준의 DFD에서 상위 수준 프로세스를 하위 프로세스로 세분화하여 작성한다. 단, 무선 네트워크 공유기의 특성상 선정한 보안 프로토콜에 따라 프로세스와 데이터의 흐름이 다르므로 본 논문에서는 WPA2 프로토콜을 적용한 레벨 1 수준의 DFD를 그림 2와 같이 작성하고, 그림 3에서는 WPA3 프로토콜을 적용한 DFD를 추가로 작성하였다. 그림 2는 WPA2 보안 프로토콜을 적용하는 네트워크 공유기와 사용자와 인터넷 기기 간 DFD로써 총 3개의 신뢰 경계를 가지며 총 12개의 프로세스, 25개의 데이터 흐름을 도출하였다. 그림 3은 WPA3 보안 프로토콜을 적용한 경우의 DFD를 나타낸 것으로 사용자와 인터넷 기기 간의 데이터 흐름은 그림 2와 동일하며 인터넷 기기와 무선 네트워크 공유기간의 DFD를 분석하였다.

3.3 STRIDE를 이용한 위협 식별 결과

3.2에서 네트워크 공유기의 데이터 흐름을 확인하고, 이를 통해 발생할 수 있는 위협을 도출하기 위해 STRIDE를 이용하였다. STRIDE에서 도출되는 각 요소는 위협 유형(Threat Type)이라고 부르며, 유형 별 관련 보안 속성 및 내용은 표 2와 같다.

STRIDE를 이용하여 그림 2, 3에서 분석한 DFD 각 요소 별 위협을 표 3과 같이 도출하였다. 식별된 위협(Threat) ID는 이후 나올 Attack Tree의 식별자로 사용된다.

3.4 STRIDE 분석을 통한 Attack Tree 및 시나리오 작성

STRIDE 분석을 통해 산출된 위협을 기반으로 공격자의 공격 의도와 공격 목표 달성을 위한 작업을 체계적으로 식별하기 위해 Attack Tree를 작성한다. Attack Tree는 다양한 Attack을 기반으로 시스템 보안을 설명하는 공식적이고 체계적인 방법이다. 기본적으로 Root 노드를 목표로 하고 해당 목표를 달성하는 다양한 공격 방법을 파생되는 Leaf 노드로 작성하여 시스템에 대한 공격 시나리오를 체계적으로 분류하여 작성할 수 있다.[11]

네트워크 공유기 공격자의 공격 목표에 대한 Attack Tree는 3가지로 작성하였으며 분류된 공격 항목은 A 식별자를 부여하였다. 또한, 3.3 절에서 STRIDE를 통해 분석한 위협들을 해당되는 각 공격에 매핑 하여 그림에 나타내었다.

먼저, 첫 번째 공격은 허가되지 않은 공격자가 네트워크 공유기에 비정상적으로 접근하는 방식의 공격이다. 가장 궁극적인 네트워크 공유기의 공격 목적으로

표 2. STRIDE 모델
Table 2. STRIDE Model

STRIDE	Description
Spoofing	Pretending to be something or someone you are not.
Tampering	Modifying something you're not supposed to modify.
Repudiation	Claiming you didn't do something (regardless of whether you did or not).
Information	Exposing information to people who are not authorized to see it.
Denial of service	Preventing system to provide service by exhausting resources.
Elevation of privilege	Allowing program or user to do things that they're not supposed to do.

그림 4는 네트워크 공유기에 비정상적으로 접근했을 경우의 Attack Tree를 나타낸다. 이는 직접적으로 네트워크 공유기의 비밀번호를 공격하는 방법, 부채널 공격을 통해 네트워크 공유기의 비밀번호를 간접적으로 공격하는 방법, 접근 권한을 획득하는 3가지로 나누어진다.

네트워크 공유기의 비밀번호를 공격하는 방법은 무작위로 암호를 대입하는 방식(brute force)과 사전공격 방식(dictionary attack)을 통해 비밀번호를 크랙하여 이를 획득하는 방법, 직접적으로 또는 네트워크 통신 데이터를 스니핑하여 비밀번호를 훔치는 방법, 비밀번호 인증을 우회하는 방법이 있다.

부채널 공격을 통해 암호를 크랙하는 방법은 알고리즘의 약점을 찾거나 무차별 공격을 하는 대신 소요시간 정보, 메모리 정보 등 시스템 파괴를 위해 악용할 수 있는 추가 정보를 기반으로 암호를 공격하는 것이다.[25]

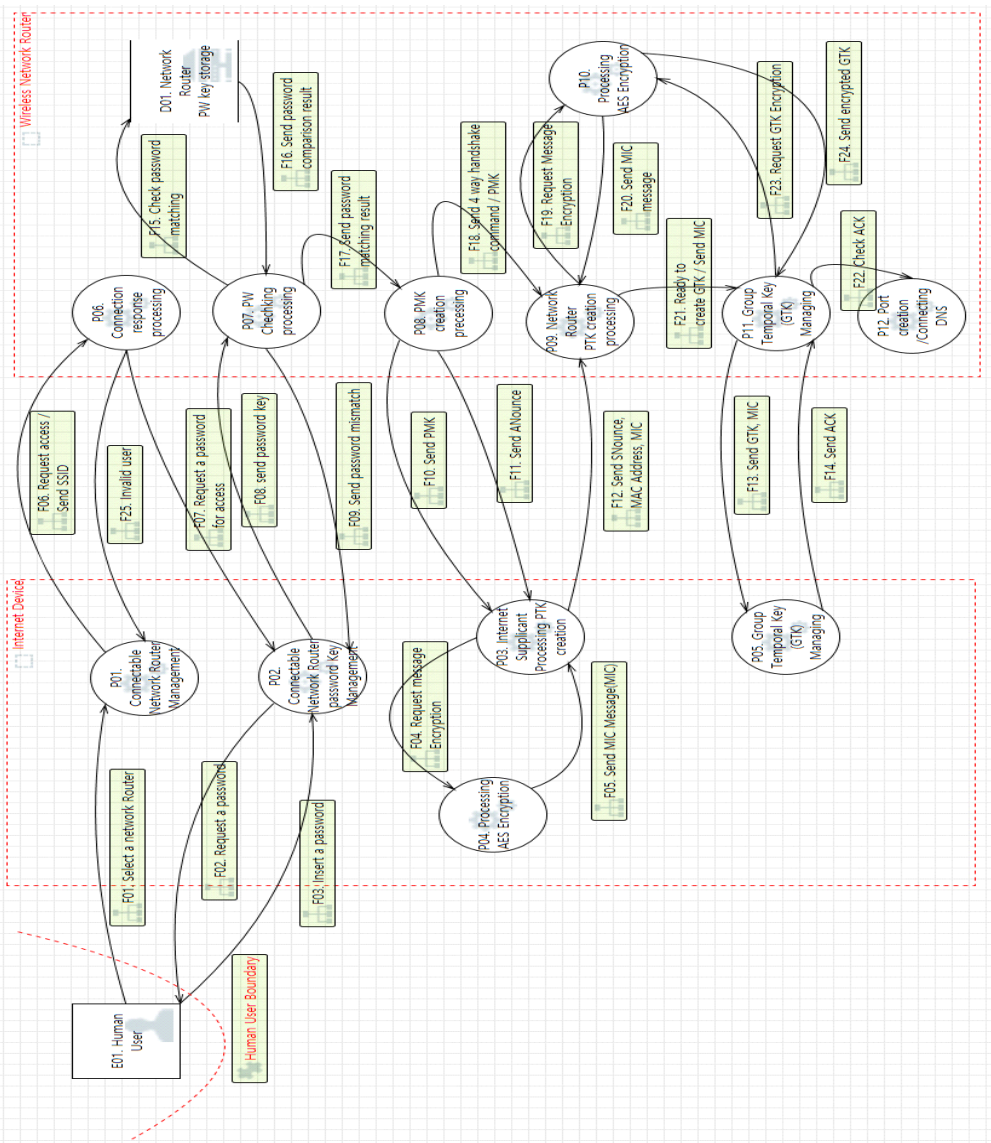


그림 2. 무선랜 공유기 Level 1 데이터 흐름도(WPA2)
Fig. 2. Wireless Network Router Level 1DFD(WPA2)

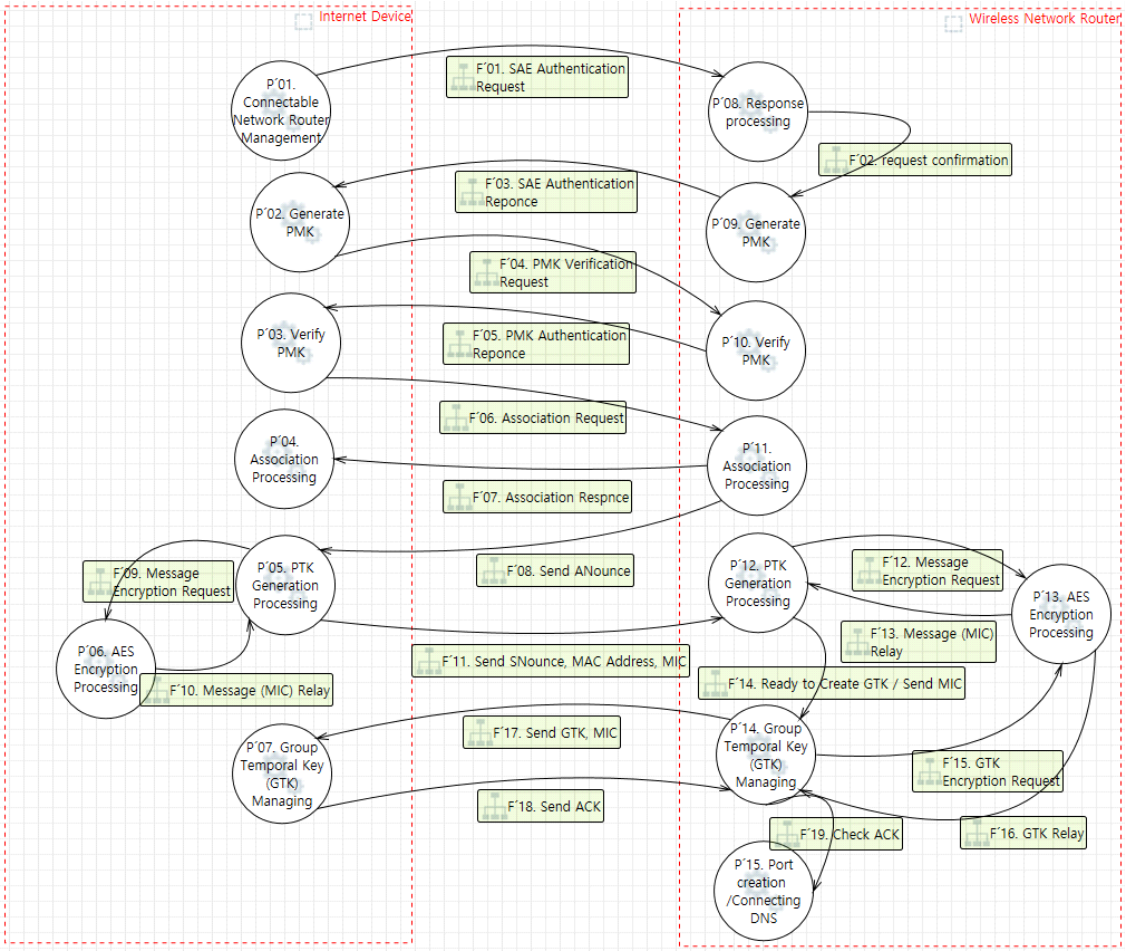


그림 3. 무선랜 공유기 Level 1 데이터 흐름도(WPA3)
Fig. 3. Wireless Network Router Level 1DFD(WPA3)

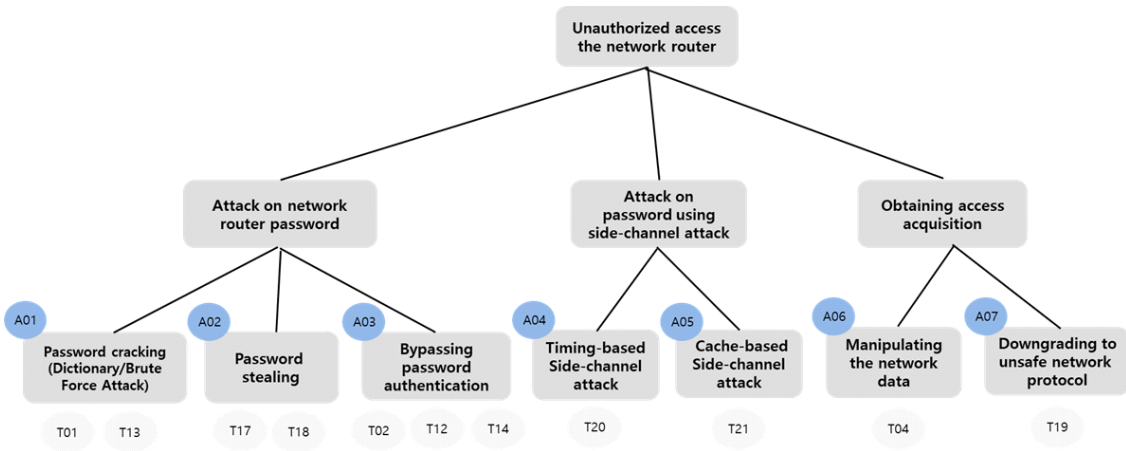


그림 4. 권한이 없는 사용자의 무선 공유기 접속 Attack Tree
Fig. 4. Unauthorized access the network router Attack Tree

표 3. 무선랜 공유기에 대한 STRIDE 분석
Table 3. STRIDE Analysis on Wireless Network Router

DFD ID	Threat ID	Threat Type	Description
F03 P02	T01	S	Use Dictionary Attack to find out the password by entering the password of a network router that is frequently used. Network routers are particularly vulnerable to Dictionary Attack because each product has a password that is initially set.
F08 F15 F16 D01	T02	I	If you do not specify a password for the network router, all anonymous users can access the network router using the frequency. This can be accessed by lots of anonymous users and degrade network performance.
F06	T03	D	When requesting a connection, it modulates an invalid SSID value through Man in the Middle Attack. This may restrict access to the network router.
F06	T04	E	When requesting a connection, an attacker can tamper with the SSID with administrator privileges through Man in the Middle Attack. Through this, an attacker can gain administrator privileges.
F01 F06 P01	T05	D	A DDOS(Distribute Denial of Service) attack can cause the network router to send connection requests that cannot be processed in time, reducing performance.
F22 P12	T06	D	It transmits an ACK value indicating that the connection is complete to the network router to create a large number of unnecessary communication ports. This may be a factor in the performance degradation of the network router.
F05 F12 P03 P09	T07	T,S	By regenerating the PTK(Pairwise Transient Key) of the Internet device/ network router in the 4-way handshake, it is possible to enable a snoofing attack in which an attacker peeks at data transmitted over the network. (CVE-2017-13077[24])
F12 F21 F13 P11 P05	T08	T,S	By regenerating the GTK(Group Key Handshake) of the Internet device/ network router in the 4-way handshake, it is possible to enable a snoofing attack in which an attacker peeks at data transmitted over the network. (CVE-2017-13078)
F13 F23 F24	T09	T,S	In the third stage of the 4-way handshake, GTK and MIC(Message Integrity Code), if data is manipulated during AES encryption, AES encryption may be broken. (KRACK) This can be used to enable snoofing attacks that peek at data by sending a forged GTK to an Internet device.
P12	T10	T	An attacker creates a communication port by performing remote access to the network router and alters the address when connecting to DNS. In this case, the Internet device user can access the Farming App or the Farming web site.
P12	T11	T,D	If an attacker sets an invalid value when creating a communication port, all users using the network router will not be able to use the network even after connection is complete.
F03 D01	T12	S	An attacker can perform an Offline Guessing Attack by acquiring the network router password hash table managed by the network router.
F02 F03	T13	S	An attacker can find out the password by conducting an Online Guessing Attack that examines all passwords and enters all possible passwords.
P07	T14	S	An attacker can perform Stolen Verifier Attack by manipulating the process that performs password authentication. This allows an arbitrary password to be successfully authenticated, so access can be allowed to a large number of unspecified persons.
F08	T15	T,D	An attacker can manipulate the password data transmitted from the Internet device with Man in the Middle Attack to return a mismatch error even if the correct password is entered.

DFD ID	Threat ID	Threat Type	Description
F10	T16	T,D	When PSK(public key) is transmitted after matching network router password, it can lead to failure in performing 4-way handshake by falsifying the data with Man in the Middle Attack. When PSK(public key) is transmitted after matching network router password, it can lead to failure in performing 4-way handshake by falsifying the data with Man in the Middle Attack.
F03	T17	I	When a user enters a password in a public place, the password may be exposed.
F08	T18	S	You can access the network router by sending the same password data by sniffing the data that the password entered by the user is transmitted to the network router.
F01 F06 F07 P01 P06	T19	T,S	When requesting a connection with WPA3 protocol in transition mode, an attacker can forcibly downgrade to an WPA2 protocol through Man in the Middle Attack. By capturing the traffic generated during this connection attempt, a brute-force attack can be enabled in a 4-way handshake.
F′03	T20	S	During the SAE Hand-shake, which is a cryptographic-based authentication protocol before the 4-way handshake, a timing-based side-channel attack can be performed to obtain timing information responding to the commit frame for negotiation of the shared key. An attacker can use this information to perform a brute-force attack to find out the password. (CVE-2019-9494)
F′01 F′02 F′03 P′08 P′09	T21	S	Cache-based side-channel attack can be performed to acquire memory access pattern information in the commit frame for negotiation of shared key during SAE Handshake, which is a cryptographic-based authentication protocol before the 4-way handshake. An attacker can use this information to perform a brute-force attack to find out the password. (CVE-2019-9494)
F′04 F′05 P′10	T22	D	By bypassing the defense mechanism against the Denial-of-Service attack of SAE, which is a password-based authentication protocol, the process can be terminated by omitting the status validation step when processing the confirm frame. This can occur as a factor in the performance degradation of the network router.

네트워크 공유기의 비밀번호를 획득하기 위해 본 공격시나리오에서는 공유기가 commit frame에 응답하는 데 걸린 시간을 이용하여 암호를 공격하는 방법, commit frame을 구축할 때 memory access pattern을 관찰하여 패턴을 이용한 암호 공격 방법이 있다. 마지막으로 접근 권한을 획득하는 공격 시나리오는 관리자 및 사용 권한이 있는 값으로 네트워크 데이터를 변조하는 방법, 안전하지 않은 보안 프로토콜로 강제적으로 다운그레이드 시키는 방법이 있다.

두 번째 공격은 네트워크 공유기의 서비스를 망가뜨려 네트워크의 성능을 저하시키거나 서비스를 중단시키는 방식의 공격이다. 이 공격은 네트워크 공유기와 인터넷 기기 간에 송수신되는 데이터에 중점을 두지 않고 네트워크 접속 자체를 방해하는 것으로 기업이나 공공기관 등 중요 서비스를 제공하는 망뿐만 아니라 결제서비스 등의 실생활에서 꼭 필요한 서비스를 제공하는 서버 등을 공격할 경우 막대한 손실을 초래할 수 있다.

그림 5는 이 DOS(Denial of Service) 공격의 Attack Tree를 나타내며 이 공격은 공유기의 네트워크 접근을 방해하는 방법, 네트워크 공유기가 시간 내 처리하지 못하는 많은 양의 연결 요청을 보내는 방법, 공유기의 설정 값을 변조하는 방법이 있다.

공유기의 네트워크 접근을 방해하는 방법은 네트워크 송수신 데이터를 변조하여 공유기 접근을 제한하는 방법과 네트워크를 사용하려는 기기로부터 전달되

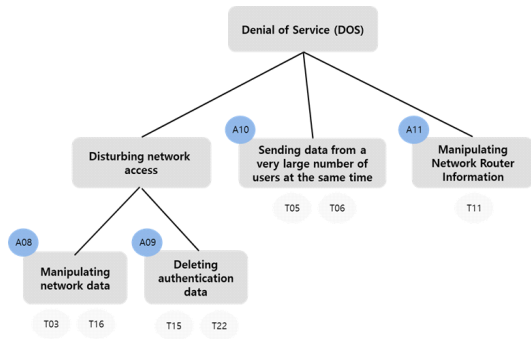


그림 5. 네트워크 공유기 서비스 거부 Attack Tree
Fig. 5. Network Router denial of service Attack Tree

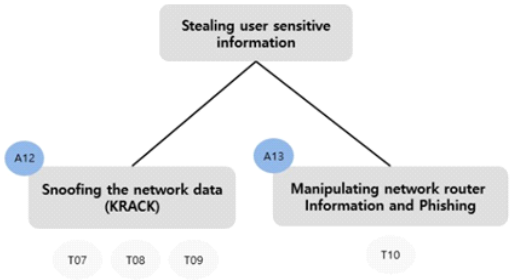


그림 6. 사용자 민감한 정보 훔침 Attack Tree
Fig. 6. Stealing User-sensitive information Attack Tree

는 인증데이터를 아예 삭제하는 방법이 있다.

세 번째 공격 방식은 사용자의 중요 데이터를 훔치는 데 목적을 둔 것으로 그림 6에서 해당 Attack Tree를 나타내었다. 이는 WPA2 보안 프로토콜을 사용하는 공유기의 경우 공격자가 네트워크 데이터를 Snooping 하는 공격이 있고, 원격으로 공유기에 접속하여 DNS 주소를 변조하여 사칭 웹사이트 등에 접근하게 하는 피싱(Phishing) 공격 방식이 있다.

3.5 DREAD를 이용한 위협 분석 결과

Attack tree를 통해 공격 시나리오가 작성된 다음 공격 시나리오별 위험 등급을 산출한다. 위험 등급이 높은 공격 시나리오에 포함된 위협은 조치하는데 높은 우선순위를 갖는다. 본 연구에서는 3.4에서 도출한 공격 시나리오에 대해 DREAD 모델[26]을 적용하여 공격 시나리오별 위험도를 분석하였다. DREAD 모델은 평가하고자 하는 대상을 DREAD의 각 요소별로 점수를 합산해 위험 등급을 정량적으로 산출하는 위험평가 방법 중 하나로 각 요소에 대한 설명은 표 4와 같다. 위험 점수는 OpenStack 프로젝트[27]에서 제시한 요소별 점수 부여 기준을 인용하였으며 점수 범위는 1점-5점으로 선정하였다. 각 요소별 점수가 1점에 가까울수록 공격 시나리오의 위협 영향이 적고, 반대로 5점에 가까울수록 위협의 영향이 크다는 것을 의미한다. 각 항목별로 부여한 점수의 총합이 분석 대상인 공격 시나리오별 위험도가 된다.

위험 대책은 위험 회피, 전가, 감소, 수용 4가지 대처 방식[11]을 고려할 수 있으나 본 논문에서는 위험을 대응하는 방안으로 감소와 수용만 채택하였다.

◎ 위험 감소(Risk Reduction) : 위험 결과 또는 발생 가능성을 낮추는 대책 수행
◎ 위험 수용(Risk Retention) : 현재의 위험을 받아들이고 잠재적 손실 비용을 감수하는 것

표 4. DREAD 모델
Table 4. DREAD Model

DREAD	Description
Damage	What will be the impact on exploitation?
Reproducibility	What is the ease of recreating the attack/exploit?
Exploitability	What minimum skill level is needed to launch?
Affected Users	How many users will be potentially impacted?
Discoverability	What is the ease of finding the vulnerability?

회피 방법은 위험을 조치하는데 필요한 비용 또는 자원이 너무 커서 그 기능을 포기하는 방법이지만 본 논문에서 분석한 네트워크 공유기는 그 기능을 하는데 필수적인 요소만 분석을 했기 때문에 제외할 기능이 없었다. 또한 전가 방법은 보험과 같이 그 위험에 대한 책임을 제 3자와 공유하는 것으로 위험을 조치하는데 특수성이 있어 배제했다.

표 5는 DREAD 분석 결과를 나타낸다. 위험의 등급(Rating)을 그룹화하기 위해 총합이 19-25점인 위협을 높은(High) 위험 등급으로, 12-18점을 중간(Medium) 위험 등급으로, 5-11점을 낮은(Low) 위험 등급으로 분류했다.

높은 위험 등급으로 분석된 A01, A02는 허가받지 않은 공격자가 다양한 방법으로 비밀번호를 크랙하여 네트워크 공유기에 접근하는 경우로서 위험 등급이 높아서 위험을 감소시키는 활동이 꼭 필요하다. 네트워크 공유기의 비밀번호 등 기본 설정 값은 복잡도가 높도록 설정하고, MAC 주소 필터링 등의 기능을 사용하여 승인된 사용자만 액세스할 수 있도록 제한한다. 또한 네트워크 데이터를 강력하게 암호화할 수 있는 프로토콜을 사용하면서도 항상 최신의 패치를 유지할 수 있도록 하여 위험을 감소시켜야 한다. 물론 사용자가 이런 무선 네트워크 보안을 지원하는 네트워크 공유기를 선정하는 것도 중요하지만, 공유기 제조업체에서도 보안을 위한 장치의 SW 및 펌웨어에 대한 주기적인 업데이트와 패치가 필요하다.

A10의 경우에는 대규모 DDoS 공격에 대응하기 위한 자체 인프라를 구축하기에는 비용 측면에서 현실적으로 한계가 있다. 반면 공격의 목적이 단순 개인의 네트워크 라우터를 대상으로 하는 경우는 희박하므로 최소한의 방어 장치로써 대응 프로세스[28]에 대

표 5. DREAD 위험도 분석.
Table 5. DREAD Threat Analysis

ID	Threat		D	R	E	A	D	Sum	Rating	Risk
A01	Unauthorized access the network router	Password cracking	3	5	3	5	3	19	High	Reduction
A02		Password stealing	3	4	3	5	4	19	High	Reduction
A03		Bypassing password authentication	3	3	1	5	1	14	Medium	Reduction
A04		Timing-based Side-channel attack	3	3	1	3	1	11	Low	Retention
A05		Cache-based Side-channel attack	3	3	1	3	1	11	Low	Retention
A06		Manipulating the network data	3	3	2	3	2	13	Medium	Reduction
A07		Downgrading to unsafe network protocol	3	3	1	5	1	13	Medium	Reduction
A08	Denial of Service(DOS)	Manipulating the network data	3	3	1	2	1	11	Low	Retention
A09		Deleting authentication data	4	2	1	3	1	11	Low	Retention
A10		Sending data from a very large number of users at the same time	4	4	4	5	4	21	High	Reduction
A11		Manipulating Network Router Information	3	2	1	5	3	14	Medium	Reduction
A12	Stealing user sensitive information	Snoofing the network data (KRACK)	5	3	1	2	4	15	Medium	Reduction
A13		Manipulating network router information and Phishing	5	3	3	2	4	17	Medium	Reduction

한 준비가 필요하다.

위험 등급이 중간인 위협들은 대처 방식을 선택적으로 적용할 수 있다. A03, A06, A07은 중간 위험 등급으로 발생 확률은 낮지만, 발생 시 영향을 받는 피해자 또는 피해 규모가 크기 때문에 서비스 식별자(SSID)를 숨기거나 방화벽을 설치하고 스파이웨어와 같은 악성프로그램을 탐지하는 백신을 사용하는 등의 위험 감소 활동을 할 수 있다. A12는 WPA2 암호화 프로토콜에서 발생한 취약점으로 이를 보완한 WPA3 프로토콜을 사용하여 위험을 감소할 수 있지만 WPA3를 쓰더라도 WPA2로 연결하도록 강제로 다운그레이드 할 수 있어 안전한 암호화 프로토콜을 사용할 수 있도록 기술적인 보완이 필요하다.

A04, A05, A08, A09는 DREAD 분석 결과 위험 등급이 낮으며, 공격자가 이를 발생시킬 수 있는 확률이 낮고, 발생 시 피해의 규모가 크지 않아 위험을 수용한다.

Ⅳ. 체크리스트 도출

3장까지 DFD, STRIDE, Attack Tree 등 위협모델링 절차에 따라 무선 네트워크 공유기의 위협을 식별하고 공격 시나리오를 도출해 보았다. 일반적으로 기기의 취약점을 점검할 때는 분석가만의 노하우를 이용하거나, 알려진 체크리스트를 이용하여 점검을 진행한다. 그러나 이러한 체크리스트들은 내용이 포괄적이거나 점검 대상에 대한 다양한 공격을 고려하고 있지 않아 체계적인 점검이 어렵다. 이런 점을 보완하기 위해 본 논문에서는 STRIDE 위협모델링을 적용하여 식별한 위협목록과 추가로 무선 네트워크 공유기 관련 자료 수집 및 발표된 보안 위협들을 포함하여 체크리스트를 도출하였다.[2,5,29,30,31,32,33] 실제 취약점이 발생할 수 있는 공격 벡터는 애플리케이션, 네트워크, 하드웨어, 시스템 4가지 영역으로 구분하였다. 또한, 체크리스트의 완전성 입증을 위해 식별한 위협 목록을

표 6. 체크리스트
Table 6. Check List

Type	Surface	Check List No.	Details	Threat No.
Application	User Authentication	C01	Confirm that router only accepts strong passwords that require authentication (eg at least 8 characters including uppercase and lowercase letters, numbers, special symbols, alphanumeric characters).	T01
		C02	Confirm that rules Including password length, disallowed character information for generating passwords are explained.	T01
		C03	Confirm that the router password uses a safe mechanism for making password.	T01
		C04	Confirm a period of changing password.	T02
		C05	Check a default initial password is set.	T02
		C06	Check that a user change the SSID and password given by the manufacturer.	T03, T04
		C07	Confirm you are limited to one login at a time when logging in.	T05
		C08	Check number of login attempts limit	T05, T13
	Web User Authentication	C09	Router web application is not vulnerable to web application vulnerabilities. (Example: Cross-Site Scripting (XSS), SQL Injection, and Cross-site request forgery (CSRF), etc.)	T01, T13
		C10	Router web application only accepts strong passwords that require authentication (eg at least 8 characters including uppercase and lowercase letters, numbers and letters).	T01, T13
		C11	Router web application rejects input with invalid or malformed data.	T14
		C12	Router web application have CAPTCHA authentication to prevent automatic attacks at login.	T14
		C13	Router web interface have management policy for authentication (login ID, log out, timeout setting, etc)	T14
	Session	C14	Router web application automatically logs the user out when the session times out.	T17
	HTTPS	C15	Router web interface only uses the encrypted HTTPS protocol.	T15
		C16	Confirm that the router web interface should restrict administrator access to HTTPS.	T15
Network	Wireless Encryption Protocol	C17	The wireless encryption is supported by the wireless network protocol with the highest security strength (eg WPA3 or at least WPA2 Enterprise (WPA/WPA2-AES)).	T09, T19, T20
		C18	When providing WPA2 protocol, TKIP option is not provided as data confidentiality protocol.	T09
	Remote administration	C19	In the initial setting, the remote administration function should be disabled.	T10
		C20	Remote administration is provided only through HTTPS.	T10
		C21	Logon restriction policies such as ID, password, and timeout for remote administration should be established and functions should be provided.	T10

Type	Surface	Check List No.	Details	Threat No.
Network	UPnP	C22	When providing the UPnP (Universal Plug and Play) function, it should be disabled by default.	T11, T12
		C23	When providing the UPnP (Universal Plug and Play) function, UPnP-UP must be supported to perform authentication between the device and the application.	T11, T12
	Port Fowarding	C24	When port forwarding, a function to restrict to source IP and source IP subnet must be provided.	T07, T08, T16
	GUEST Network	C25	Provide a GUEST Network and set it to separate from the main local network.	T07, T08, T16
	DoH/DoT	C26	New secure DNS, DNS over HTTPS (DoH) and DNS over TLS (DoT), should be provided as options.	T10
	WPS	C27	Remove Wi-Fi Protected Setup (WPS) or Turn Off	T02
System	Firewall	C28	The router must provide security through a firewall.	T06, T11, T12
		C29	The router firewall should consider all open ports as inbound rules for WAN/Internet.	T11, T12, T20, T21
		C30	The router firewall must consider all open ports as inbound rules to the LAN.	T11, T12, T20, T21
	Shell Interface	C31	Telnet and SSH must be disabled.	T07, T08, T20, T21
	Vulnerability Management	C32	A manufacturer or developer provides an official channel (such as a product website) for the disclosure of device vulnerabilities and related information.	-
		C33	A manufacturer or developer provides an official channel for security patching software (e.g. product website)	-
		C34	Users can verify the authenticity of software/firmware/patch files by verifying digital signatures or file checksums.	-
		C35	The device management platform allows you to deploy software/firmware/patches to connected devices.	-
	Data and Event Monitoring	C36	Monitor audit logs and security event logs for firmware updates	-
		C37	Security-related events such as privilege escalation attempts should be well defined and logged.	-
		C38	Monitor and identify anomalies with security events.	-
		C39	Write permission to the security audit log should be granted only to administrators.	-
		C40	Provide a list of all devices connected to the router.	-
Hardware	Firmware acquisition	C41	Obtaining software/firmware/patch files through official webpage	-
		C42	Support updating device software/firmware using official software tools	-
	Tampered Firmware	C43	verify the integrity of software/firmware/patch files by verifying digital signatures or file checksums	-
		C44	Restrictions on updating forged/falsified software/firmware/patch files	-

Type	Surface	Check List No.	Details	Threat No.
Hardware	Unauthorized port	C45	Restriction of interworking of management functions through physical interfaces or ports	-
		C46	Remove or disable unnecessary physical external interfaces or ports	-
	Debug Interface	C47	Remove or disable unnecessary Debug interface	-
		C48	Requires authentication or access control when using the debug interface or port	-

각 체크리스트의 항목과 연관 지어 표현하였으며, 그 결과는 표 6과 같다.

V. 결 론

무선 네트워크 공유기는 모바일, 스마트 기기 시장이 증가함에 따라 서서히 그 사용이 확대되었으며, 최근 비대면 수요 증가로 사회의 필수재로 인식되고 있다. 그에 반해 무선 네트워크 공유기의 보안 위협에 대한 인식은 높지 않아 공격자에 의한 악의적인 해킹, 사생활 침해와 같은 보안 사고가 발생할 가능성이 높으며 그 피해 규모가 클 것으로 예상된다. 따라서 본 논문에서는 위협 모델링을 이용하여 체계적인 무선 네트워크 공유기의 위협을 분석하고 도출한 모든 결과를 기반으로 무선 네트워크 공유기에 대한 보안 점검을 할 수 있는 체크리스트를 도출하였다.

무선 네트워크 공유기의 보안 프로토콜, 사용자 인증 방법과 같은 세부적인 사항은 무선 네트워크 공유기의 특성에 따라 다르게 구현할 수 있다. 본 논문의 체크리스트를 활용하면 무선 네트워크 공유기의 모든 Attack Surface에서 빠짐없이 보안 기능을 지원하고 있는지 점검이 가능하다. 또한 추후 안전한 무선 네트워크 공유기 사용 환경을 구축하는 데 기여할 것으로 사료된다. 향후 신규 보안 프로토콜 및 이를 탑재한 무선 네트워크 공유기가 출시될 것이기 때문에 새로운 유형의 위협 및 공격이 발견될 때 위협 모델링은 지속적으로 이루어져야 할 필요가 있다.

References

[1] Norton, *NORTON WI-FI RISK REPORT*, Retrieved Apr. 20, 2022, from https://www.nortonlifelock.com/us/en/newsroom/press-kits/norton-wifi-risk-report-2017.

[2] H. R. Bae, M. Y. Kim, S. K. Song, S. G. Lee, and Y. H. Chang, “Security attack analysis for wireless router and free wi-fi hacking solutions,” in *JCCT*, vol. 2, no. 4, pp. 65-70, Nov. 2016. (http://dx.doi.org/10.17703/JCCT. 2016.2.4.65)

[3] J. Fitzpatrick, *The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords*, Retrieved Aug. 23, 2021, from https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters.

[4] M. Vanhoef and F. Piessens, “Release the Kraken: New KRACKs in the 802.11 Standard,” *ACM SIGSAC Conf. CCS ’18*, Toronto, Canada, 2018. (https://doi.org/10.114 5/3243734.3243807)

[5] Wi-Fi Alliance, *Wi-Fi certified WPA3*, Retrieved Jun. 2018, from https://www.wi-fi.org/discover-wi-fi/security.

[6] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security : Technical challenges, recent advances and future trends,” in *Proc. IEEE*, vol. 104, no. 9, pp. 1727-1765, Sep. 2016. (https://doi.org/10.1109/JPROC.2016.2558521)

[7] M. Waliullah and D. Gan, “Wireless LAN security threats & vulnerabilities,” in *IJACSA*, vol. 5, no. 1, pp. 176-183, Jan. 2014. (https://doi.org/10.14569/IJACSA.2014.050125)

[8] A. K. Mohan and M. Sethumadhavan, “Wireless security auditing: Attack vectors and mitigation strategies,” in *7th ICACC-2017*, pp. 674-682, Cochin, India, Aug. 2017. (https://doi.org/10.1016/j.procs.2017.09.153)

[9] Microsoft, *Threat Modeling*, Retrieved Jul. 22, 2021, from https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling.

[10] Microsoft, *Microsoft Threat Modeling Tool 2016*, Retrieved Jul. 21, 2021, from https://aka.ms/threatmodelingtoolx?id=491.

[11] S. Adam, *Threat Modeling Designing for Security*, 1st Ed., Wiley, 2014.

[12] Microsoft, *The Threats to Out Products*, Retrieved Aug. 27, 2009, from https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/

[13] K. Wuyts, D. V. Landuyt, A. Hovsepyan, and W. Joosen, "Effective and efficient privacy threat modeling through domain refinements," in *Proc. 33rd Annu. ACM SAC '18*, pp. 1175-1178, New York, USA, Apr. 2018. (https://doi.org/10.1145/3167132.3167414)

[14] T. UcedaVelez and M. M. Morana, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*, John Wiley & Sons, Inc., May 2015.

[15] P. Saitta, B. Larcom, and M. Eddington, *Trike v.1 Methodology Document [Draft]*, Jul. 13, 2005 from http://www.octotrike.org/papers/Trike_v1_Methodology_Document-draft.pdf.

[16] Microsoft, *The STRIDE Threat Model*, Retrieved Jul. 21, 2021, from https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

[17] S. Nataliya, *Threat Modeling: 12 Available Methods(2018)*, Retrieved Aug., Apr. 5, 2022 from https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/.

[18] M. Tasch, R. Khondoker, R. Marx, and K. Bayarou, "Security analysis of security applications for software defined networks," in *Proc. AINTEC 2014 on Asian Internet Eng. Conf.*, ACM, 2014. (https://doi.org/10.1145/ 2684793.2684797)

[19] A. Hadding and Dr. J. Zalewski, "Threat modeling in embedded systems," Florida Gulf Coast University, 2012

[20] E. J. Park and S. J. Kim, "Derivation of security requirements of smart factory based on STRIDE threat modeling," *Conf. KIISC*, vol. 27, no. 6, Dec. 2017. (https://doi.org/10.13089/JKIISC.2017.27.6.1467)

[21] J. S. Lee, S. Y. Kang, and S. J. Kim, "Study on the AI speaker security evaluations and countermeasure," *Conf. KIISC*, vol. 28, no. 6, Dec. 2018. (https://doi.org/10.13089/JKIISC.2018.28.6.1523)

[22] B. U. Hong, S. M. Lee, M. S. Park, and S. J. Kim, "Threat-based security analysis for the domestic smart home appliance," *KIPS Trans. Comput. and Commun. Syst.*, vol. 6, no. 3, pp. 143-158, Dec. 2016. (https://doi.org/10.3745/ KTCCS.2017.6.3.143)

[23] L. Sion, K. Yskout, D. Van Landuyt, and W. Joosen, "Solution-aware data flow diagrams for security threat modeling," in *Proc. 33rd Annu. ACM SAC '18*, NY, USA, 2018. (https://doi.org/10.1145/3167132.3167285)

[24] MITRE, *Common Vulnerabilities and Exposures*, Retrieved Jul. 22, 2021, from https://cve.mitre.org.

[25] H. B. Kim and H. S. Kim, "Side-channel analytics security conference research trends examined by CHES 2020," *Conf. KIISC*, vol. 30, no. 6, pp. 67-81, Dec. 2020.

[26] M. Howard and D. Leblanc, *Writing Secure Code*, 2nd Edition, Microsoft Press, Dec. 2002.

[27] OpenStack project, *Security/OSSA-Metrics*, https://wiki.openstack.org/wiki/Security/OSSA-Metrics#DREAD

[28] Korea Int. & Sec. Agency (KISA), *DDos Attack Response Guide*, Aug. 2021, https://www.krcert.or.kr/filedownload.do?attach_file_seq=3168&attach_file_id=EpF3168.pdf

[29] Korea Int. & Sec. Agency (KISA), *Security Guide to be applied for Router products*, Feb. 2021, https://boho.or.kr/data/guideView.do?bulletin_writing_sequence=22943

[30] CISA, *Security Tip (ST05-003) Securing Wireless Networks*, May 08, 2020, https://www.cisa.gov/uscert/ncas/tips/ST05-003

[31] HKCERT, *IoT Device(Wi-Fi) Security Study*, Mar. 2020, https://www.hkcert.org/f/blog/263544/95140340-8c09-4c9a-8c32-cedb3eb26056-DLFE-14407.pdf.

[32] SECURELIST by Kaspersky, *Router security in 2021*, Jun. 8, 2021, https://securelist.com/router-security-2021/106711/

[33] P. Kim, S.-B. Moon, and Y.-H. Lee, "Risk analysis for ways of choosing passwords in public access points," in *JKIIT*, vol. 15, no. 1, pp. 63-70, Jan. 31, 2017. (https://doi.org/10.14801/jkiit.2017.15.1.63)

강 수 진 (Su-jin Kang)

2008년 2월 : 경북대학교 전자전기컴퓨터 학부 졸업

2008년 3월~현재 : LIG 넥스원 지능형SW연구소 선임연구원

<관심분야> 무기체계 SW 테스팅, SW 보안

[ORCID:0000-0001-8950-6910]

조 현 석 (Hyun-suk Cho)

2014년 2월 : 한성대학교 컴퓨터공학과 학사

2020년 2월 : 고려대학교 정보보호대학원 석사

2014년 3월~현재 : LIG 넥스원 지능형SW연구소 선임연구원

<관심분야> 무기체계 SW 테스팅, SW 보안

[ORCID:0000-0002-4420-6719]

신 영 섭 (Young-seop Shin)

2007년 2월 : 충남대학교 전자전파정보통신 학사

2009년 2월 : 충남대학교 전자전파정보통신 석사

2009년 1월~현재 : LIG 넥스원 지능형SW연구소 수석연구원

<관심분야> 무기체계 SW 테스팅, SW 보안

[ORCID:0000-0002-2528-0139]

조 규 태 (Kyu-tae Cho)

2002년 2월 : 숭실대학교 컴퓨터학부 학사

2004년 2월 : 한국과학기술원 전산학과 석사

2007년 2월 : 한국과학기술원 박사 수료

2007년 2월~현재 : LIG 넥스원 지능형SW연구소 수석연구원

<관심분야> 무기체계 SW 테스팅, 인공지능, 머신 러닝, SW 설계