무선 공유기별 초기 패스워드 보안 수준 분석과 이에 따른 무선 공유기 패스워드 패턴 및 보안 수준 강화에 관한 연구

김종식* 조재현* 최예지* 염정현**

중부대학교

A Study on the Analysis of Initial Password Security Level by Wireless Router, thereby strengthening the Password Pattern and Security Level of Wireless Router

JongSik Kim* JaeHyeon Cho* YeJi Choi* JeongHyun Yeom**

Joongbu University

요 약

본 논문은 현재 공공장소에서 사용하는 비율이 높은 공유기들의 초기 패스워드 패턴을 분석하여 환경을 구성한 뒤 무차별 대입 공격을 수행한다. 이후 무차별 대입 공격의 수행 시간을 자료로 하여 각 패턴의 초기 패스워드의 안전성을 분석하며 이에 따른 각 공유기의 보안 수준에 대하여 정의한다. 또한, 분석 자료를 바탕으로 패스워드의 안전성을 높이기 위한 패스워드 설정 방법을 연구, 제시하며 보안 수준을 높이는 데 필요한 무선 공유기 초기 네트워크 보안 설정 방식에 대해 제시한다.

I. 서론

본 논문은 현재 공공장소에서 사용하는 비율이 높은 공유기들에 설정된 초기 패스워드에 대한 무차별 대입 공격을 수행해 수행 시간을 기반으로 초기 패스워드의 보안 수준을 파악, 분석하여, 무차별 대입 공격에 대하여 안전한 패스워드 설정 방법 및 보안 설정 방법에 대해 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 현재 공공장소에서 가장 많이 사용하고 있는 3가지 종류 공유기(A사, B사, C사)의 초기 패스워드를 분석한 뒤 정리한다. 3장에서는 2장에서 정리된 각 공유기의 초기 패스워드 패턴을 사용하여 3가지 종류의 GPU를 사용하여 초기 패스워드별 무차별 대입 공격을 수행한 뒤 수행 시간을 정리하여 이를 바탕으로 평균적 성능으로 주로 사용하는 무선 공유기들의 초기 패스워드를 알아내는 데 필요한 무차별 대입 공격의 수행 시간을 예측한다. 4장에서는 3장의 연구 결과를 바탕으로 무차별 대입 공격에 대하여 안전한 패스워드 패턴을 제시하며 이에 따라 무선 공유기의 초기 네트워크 설정 방식별 보안 수준을 분석하며 더 나은 보안 설정 방법을 제시한다. 5장에서는 결론을 내며 본 논문을 끝낸다.

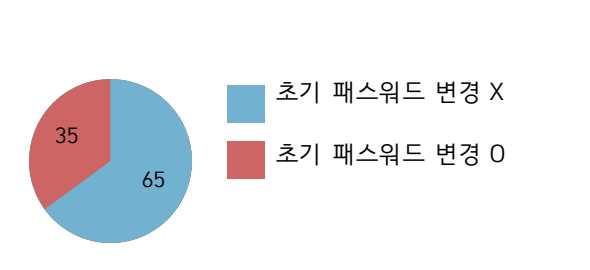
II. 자료 분석

현재 공공장소에서는 통신사의 인터넷 공유기를 사용하는 곳이 많다. 연구에 앞서 이를 검증하기 위해 지하철역, 카페, 학원 등을 포함한 총 50곳에 대해 공유기 사용 비율을 조사해 보았다. 통신사 공유기 사용 비율은 다음[표 1]과 같았다. 총 50곳 기준으로 22곳이 A사, 19곳이 B사, 6곳이 C사, 3곳이 기타 업체를 이용하였다. 동시에 초기 패스워드를 변경 사용 여부에 관해서도 조사[표 2]해 보았다.

[표 1] 공공장소에서의 각 공유기 비율(총 50곳)

A사	B사	C사	기타
44%	38%	12%	6%

[표 2] 공유기 초기 패스워드 변경 비율 (%)



조사 결과 초기 패스워드를 변경하여 사용하는 경우는 35%이며, 이 경우 패스워드의 복잡성(길이 10자리 이상, 특수문자 포함)을 조사해 보았을 때 안전한 패스워드를 위한 패스워드의 복잡성을 만족하는 경우는 전체 표본에서 10% 도 되지 않는 수치를 보였다. 이를 통해 대부분 공유기가 통신사에서 설정한 초기 비밀번호를 사용하며 변경하더라도 복잡성이 높지 않은 공유기가 대부분이라는 사실을 알 수 있다. 초기 패스워드를 그대로 사용할 경우 무차별 대입 공격에 대한 위험성을 제시하기 위하여, 각 공유기의 초기 패스워드의 패턴을 정리해보았다.

2.1 A사 공유기

A사 공유기의 초기 패스워드는 총 10자리로 구성되어 있으며 제조번호의 마지막 숫자 3자리를 패스워드의 마지막 숫자 3자리로 사용하며 앞의 7자리는 임의의 숫자 + 알파벳 소문자를 채택하여 사용하였다. 이때 알파벳 소문자의 경우 a ~ l + x, y, z 범위의 알파벳을 사용하며 m ~ w 범위의 알파벳은 사용하지 않았으며 숫자의 경우 0에서 9 사이 범위의 숫자를 사용하였다.

2.2 B사 공유기

B사 공유기의 초기 패스워드는 총 10자리로 구성되어 있으며 제조번호의 숫자 10자리를 그대로 패스워드로 채택하여 사용하였다. 맨 앞자리의 숫자는 1 또는 2를 주로 사용하는 특징을 보였으며, 나머지 9자리의 경우 0에서 9 사이 범위의 숫자를 사용하였다.

2.3 C사 공유기

C사 공유기의 초기 패스워드는 총 10자리로 구성되어 있으며 제조번호의 숫자 10자리를 그대로 패스워드로 채택하여 사용하였다. 맨 앞자리의 숫자는 1에서 4 사이 범위의 숫자를 주로 사용하며, 1을 가장 많이 채택하여 사용하는 것으로 보였다. 일반적으로 이후 5자리는 0으로 채워 넣은 뒤 마지막 4자리만 0에서 9 사이 범위의 숫자를 사용하였다.

무차별 대입 공격의 경우 패스워드의 Word list의 크기와 수행 시간이 비례하기에 공유기의 초기 비밀번호의 보안 수준을 분석하기 위해 패스워드의 Word list의 크기를 비교해 보았다. 결과적으로 A사 공유기의 초기 패스워드 보안 수준이 가장 높았으며 그다음으로는 B사 공유기, 마지막으로 C사 공유기의 경우 초기 패스워드 보안 수준이 낮아 무차별 대입 공격을 통해 단시간 내에 패스워드가 노출될 가능성이 큰 것으로 예측되었다.

III. 연구 과정 및 결과

3.1 연구 과정

본 연구에서는 2장의 자료 분석 결과를 토대로 Hashcat 라이브러리를 사용하여 각 공유기의 초기 패스워드 패턴에 대하여 무차별 대입 공격을 수행하였다.

무차별 대입 공격은 8자리, 9자리, 10자리의 임의의 숫자들로 이루어진 패스워드, 추가로 C사 공유기의 초기 패스워드 총 4가지를 대상으로 수행하였으며 C사 공유기의 초기 패스워드 패턴은 2장에서 분석한 자료를 기반으로 무차별 대입 공격을 수행하였다.

무차별 대입 공격을 통하여 각 패스워드 패턴별로 수행 시간을 측정하기 위하여 GTX-1050ti, GTX-1660ti, GTX-1070 3가지 종류의 GPU를 채택하여 사용하였으며 아래의 [표 3]은 GPU 별로 Hashcat 라이브러리를 사용하여 위에서 제시한 패스워드 패턴에 대하여 무차별 대입 공격을 수행하였을 때, 필요한 최

대 수행 시간을 보여준다.

[표 3] 무차별 대입 공격 최대 수행 시간

	8자리	9자리	10자리	C사
1050ti	10m	2h	1d	6s
1660ti	4m	52m	10h	5s
1070	3m	45m	7.5h	5s

3.2 연구 결과

[표 1]에서는 적절한 성능의 GPU를 가지고 있다고 가정할 때 현재 사용하는 비율이 높은 무선 공유기들의 초기 패스워드에 대하여 무차별 대입 공격을 수행한다면 길어도 1일 이내에 무차별 대입 공격이 성공 가능하다는 것을 보여주고 있다.

C사 공유기의 경우 초기 패스워드 패턴의 무차별 대입 공격 경우의 수가 매우 적은 편이라 수 초 내에 패스워드가 노출될 확률이 매우 높은 것을 확인할 수 있으며 B사 공유기의 경우 2장의 분석 결과 초기 패스워드의 맨 앞자리에 1 또는 2를 주로 사용하는 것으로 보이기에 이러한 초기 패스워드일 경우 적으면 2시간에서 길게는 최대 1일 이내의 시간 내에 패스워드가 노출될 수 있다는 정보를 얻을 수 있었다. A사 공유기의 경우 임의의 숫자에 알파벳까지 사용하기 때문에 무차별 대입 공격을 위해 필요한 Word list가 매우 방대하여 해당 연구에선 제외하였다. 그러나 Word list의 경우의 수를 계산하여 B사 공유기와 비교해 보면 무차별 대입 공격 성공에 필요한 시간이 B사 공유기보다 약 3,000배 더 필요한 것으로 계산되었다.

최근에 출시된 GTX-3090의 경우 해당 프로그램에서 수치상 1660ti의 약 3배의 성능을 보여주며 이에 따라 8자리, 9자리, 10자리 패스워드에 대한 무차별 대입 공격 수행 시 약 1m, 15m, 2.5h의 수행 시간이 필요한 것으로 예측할 수 있으며 이 수행 시간은 더 앞으로 더욱 향상된 성능의 GPU가 출시됨에 따라 더욱 줄어들 가능성이 있다.

결과적으로는 본 논문에서 연구한 공유기들에 대하여 초기 패스워드를 변경하지 않고 그대로 사용할 경우 A사 공유기를 제외하고는 단기간 내에 패스워드가 무차별 대입 공격으로 인해 노출될 확률이 매우 높은 것을 확인할 수 있으며 A사 공유기의 경우에도 충분한 시간만 있다면 언제든 무차별 대입 공격에 노출될 가능성이 있는 것을 확인할 수 있었다.

IV. 보안 수준 강화방식 제안

4.1 사용자

연구 결과에 따르면 초기 패스워드를 그대로 사용하지만 않는다면 그것만으로도 패스워드의 안전성을 높일 수 있다는 것을 알 수 있었다.

가장 안전한 패스워드는 특수문자, 영문자, 대문자, 숫자를 사용한 10자리 이상의 패스워드를 만드는 것이다. 10자리를 기준으로 하였을 때 무차별 대입 공격을 위해 필요한 Word list의 수가 약 4.34e+19개이기 때문에 무차별 대입 공격을 통한 공격이 현실적으로 불가능한 것을 확인할 수 있으며 패스워드의 길이가 길어질수록 패스워드의 안전성은 비례하여 더 증가하게 된다.

4.2 제조사

본 연구를 통해 대상 기업들의 초기 패스워드는 분석 이후 현실적인 시간 내에 언제든지 공격당해 패스워드가 노출될 수 있다는 결론이 도출되었다. 그러나 조사 결과 제조사 측에서 초기 패스워드를 변경할 수 없도록 만들어 놓은 경우도 확인되었다. 정책상 이를 존중하더라도 기존보다 높은 보안의 초기 패스워드 패턴 설계가 필요할 것이다. 혹은 공유기 설치 시 초기 패스워드를 10자리 이상의 길이와 특수문자 등을 포함한 패스워드로 변경해야 인터넷을 사용 가능토록 설계한다면 보안 수준을 높일 수 있을 것이다.

조사 결과 현재 4.1 방법을 채택하지 않은 곳이 많이 존재한다는 사실을 알 수 있었다. 그러므로 4.2 방법이 함께 병행되어야 전반적인 무선 공유기의 보안 수준을 강화할 수 있을 것이다.

V.결론

본 연구는 현재 공공장소에서 사용하는 비율이 높은 무선 공유기의 초기 패스워드에 대하여 무차별 대입 공격을 수행해 초기 패스워드를 그대로 사용하는 경우의 위험성을 증명하였으며, 무차별 대입 공격으로 인해 노출될 수 있는 패스워드 보안 강화방식에 대해 제안하였다.

연구 결과를 바탕으로 현재 상용화되어 있는 무선 공유기의 초기 네트워크 설정 방식들에 대해 각 초기 무선 네트워크 설정 방식별 보안 수준을 분석하였으며 분석 결과를 바탕으로 가장 보안 수준이 높은 초기 무선 네트워크 설정 방식을 제시하였다.

개인 사용자의 경우 패스워드가 노출되더라도 이로 인한 치명적인 피해를 받을 가능성이 비교적 적다고 말할 수 있지만, 공공장소와 같이 무선 네트워크에 연결된 기기의 개수가 많은 장소에서 해당 무선 공유기의 패스워드가 노출된다면 ARP Spoofing 공격과 같은 중간자 공격 등에 의해 패킷의 정보가 그대로 노출될 가능성이 있으며 악의적인 목적을 가진 공격자에 의해 중요한 정보들이 노출될 가능성이 존재한다.

무선 네트워크 기술은 점점 발달하고 있으며 앞으로 무선 네트워크를 사용하는 기기들도 점점 늘어날 것으로 예상된다. 본 논문에선 가장 보완하기 쉽지만, 사용자가 쉽게 간과할 수 있는 무선 공유기의 패스워드에 대하여 근본적인 보안 수준을 높이기 위해서 이와 같은 방법을 사용하여 사용자가 미처 신경 쓰지 못한 취약점에 대하여 보완해주는 방안을 제시해 보았으며 무선 공유기의 초기 네트워크 설정 방법에 관해 제안한 방법을 도입하는 것이 필요하다고 생각한다.

[참고문헌]

[1] 강다연. "패스워드 선택이 보안효과에 미치는 영향." 국내석사학위논문 부산대학교 대학원, 2008. 부산

[2] Egelman S ,Sotirakopoulos A ,Muslukhov I ,Beznosov K ,Herley C . "Does My Password Go Up to Eleven? the Impact of Password Meters on Password Selection" CHI -CONFERENCE- : 2379-2388.

[3] 김종회(Kim Jong Hoi),안지민(Ahn Ji Min), 김민재(Kim Min Jae),and 주용식(Joo Yong Sik). "GPU에서의 SEED암호 알고리즘 수행을 통한 공인인증서 패스워드 공격 위협과 대응." 정보보호학회지 20.6 (2010): 43-50.

[4] 김경훈(KyoungHoon Kim),김승연(Seung-Yeon Kim),and 권태경(Taekyoung Kwon). "패스워드 강도 측정 방법 연구 동향." 정보보호학회지 27.1 (2017): 31-38.