802.11 WEP 유효성 검증*

김예호, 최형기
성균관대학교 전자전기컴퓨터공학부
e-mail : {yhkim, hkchoi}@hit.skku.edu

Safety verifications the inside WEP

Yae-hoe Kim, Hyoung-kee Choi
The School of Information and Communication Engineering
Sungkyunkwan University, Suwon, Korea, 440-746

요 약

무선랜을 사용한 비밀통신은 공격에 노출되기 쉽기 때문에 반드시 보안 환경이 필요하다. 보안을 위한 방법으로 IEEE 802.11 에서 제시하는 WEP (Wired Equivalent Privacy)가 사용된다. 구현이 쉽고 연산 속도가 빠르기 때문이다. 하지만 현재 WEP 를 기반으로 보호된 네트워크는 공격자에게 언제나 노출되어 있다. 이 논문에서는 WEP 의 문제점을 분석하고 이를 이용한 공격 기법을 제안하고 일반적인 환경에서 WEP 의 유효성을 실험을 통해 밝힌다.

1. 서론

무선랜은 다양한 단말과 AP(Access Point)로 구성된다. 단말은 AP에 무선으로 접속하고 AP를 통해서 서비스를 이용한다. 무선랜은 유선랜보다 강한 보안이 요구된다. 유선랜은 해당 링크에 물리적으로 접속하지 않는 한 전송되는 데이터를 이 구간에서는 접근할 수 없다. 반면에 무선랜은 송·수신 전파가 공간으로 확산되어 다른 단말기와 공유되기 때문에 공격자의 접근이 용이하다. 이러한 필요성에 의해서 IEEE 802.11 표준에서는 WEP를 제안했다. WEP는 유선랜과 동일한 수준의 보안 기능을 무선랜에서 제공하기 위해 설계된 암호기법이다. WEP는 단말기와 AP 사이의 무선 접속 구간에 보안을 제공한다.

하지만 IEEE 802.11 와 WEP는 취약점이 있다. 표준에 포함되지 않은 키 설정 프로토콜의 문제부터, RC4 (Rivest Cipher 4)알고리즘과 CRC-32(Cyclic Redundancy Check 32bits) 무결성 알고리즘의 취약점 등이 대표적이다. 이러한 WEP의 취약점을 이용하면 공격자에 의해 WEP의 비밀정보가 쉽게 해독될 수 있다.

본 논문에서는 WEP의 취약점을 바탕으로 WEP 공격 기법을 분석해서 통합적인 공격기법을 제안한다. 일반적인 환경에서 새로운 공격방법의 효율성을 실험을 통해 검증한다. 마지막으로, WEP의 유효성을 검증하고, 그에 따른 대안을 제시한다.

본 논문의 2 장은 관련 연구, 3 장은 WEP의 정의, 4 장은 취약점 분석, 5 장은 공격 기법에 대한 분석, 6 장은 구현과 실험을 보이고, 7 장에서 결론을 맺는다.

2. 관련 연구

WEP는 IEEE 802.11 표준에서 무선랜 보안을 위해서 제시하는 기법이다. WEP는 비밀성 보장을 위해서 RC4 알고리즘으로 암호화를 수행하고, 무결성 보장을 위해서 CRC-32 알고리즘을 사용한다. 자세한 WEP 알고리즘에 대해서는 3 장에서 설명한다. 본 장에서는 WEP에 관련된 연구들을 소개한다.

David Wagner와 그의 팀은 비밀키와 초기화 벡터로 생성되는 시드값이 반복 사용될 수 있음을 보이고, 무결성 알고리즘의 취약성을 증명했다.[1]

Scott Fluhrer와 그의 팀은 [2]에서 RC4 알고리즘의 구조적 약점을 이용한 FMS (Fluhrer, Mantin, Shamir) 공격을 제안했다. RC4 에 대해 설계된 FMS 공격은 WEP환경에서 매우 효율적인 방법이며, 이후 다른 공격 방법의 기반이 된다. FMS 공격을 기반으로 만들어진 프로그램으로 AirSnort이란 프로그램이 있다.

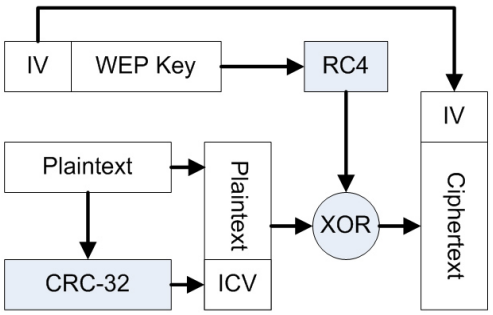
Rafik Chaabouni는 KoreK 공격을 증명하고 새로운 공격방법을 추가했다.[3] KoreK공격은 RC4 에 대한 Fluhrer의 초기화 벡터의 초기 조건에 따른 분석을 바탕으로 설계되었다.[2] 기존의 공격 기 법과 Arbough 에 의해 제안된 Inverted Attack을 포함한다. 이 공격을 이용한 AirCrack, WepLab이란 프로그램이 있다.

Andrea Bittau와 그의 팀은 [4]에서 WEP에 대한 단편화 공격을 제안했다. 이 공격은 데이터에 대한 단편화와 무결성 알고리즘의 약점을 이용한다.

Erik Tews는 Klein의 분석을 바탕으로 키 분리 기법과 유효키 검증 기법을 제안했다.[5]

이 장에서 언급한 문제점은 WEP에 대한 취약점들을 기반으로 한다. 이미 다양한 공격 방법들이 제안되고, 관련 실험이 수행되었지만 이론이 아닌 일반적인 환경에서 통합적인 모델을 제시하고 WEP의 위험성을 보인 경우는 없었다.

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음



(그림 1) WEP 암호화 과정

3. WEP

WEP는 유선과 동일한 보안 기능을 무선에서도 제공하기 위해 만든 기법이다. 단말과 AP사이의 무선구간에서 인증과 기밀성, 그리고 무결성을 보장한다.

WEP는 초기화 벡터와 비밀키로 정의된 두 가지 인자가 필요하다. 비밀키는 단말기와 AP 장비에 동일하게 저장되어 있는 값이다. 초기화 벡터는 사전 공유하지 않고 메시지에 포함되어 전송된다.

WEP는 암호 알고리즘인 RC4[9]와 무결성 알고리즘인 CRC-32 로 구성된다. RC4 의 세부적인 전개 과정은 [2]에 설명되어 있다. CRC-32 는 메세지에 대해서 고정된 길이의 CRC를 생성해서 복호화 과정에 전송 데이터의 무결성을 확인한다. WEP의 자세한 내용은 IEEE 802.11 표준[10]에 설명되어 있다.

4. WEP 취약점 분석

IEEE 802.11 표준의 취약점: 첫째, 802.11 표준에는 키 설정 프로토콜을 정의하지 않기 때문에 네트워크의 모든 단말기와 AP에 사전 공유 비밀키를 수동 설정하게 된다. 둘째, 각 단말에 유일한 키를 할당하게 하는 방법이 없기 때문에 서비스 내의 AP와 단말이 같은 키로 설정된다. 셋째, 단말이 올바른 AP를 확인할 수 있는 방법이 없는 단방향 인증만을 제공한다. 넷째, AP가 전송하는 Beacon 메시지를 통해서 AP의 정보가 전파된다.

초기화벡터 도입으로 인한 취약점: 동기 모드의 스트림 암호는 데이터 손실에 취약하다. 무선랜에서 데이터 손실은 광범위하게 확산되기 때문에, 동기화 스트림 암호는 적합하지 않다. WEP는 동기화 요구조건을 세션으로부터 패킷으로 옮겨서 문제를 해결했다. 각각의 패킷에 대해서 유일한 키를 사용하기 위해서 도입한 것이 초기화 벡터이다. 하지만 초기화 벡터로부터 많은 취약점이 발생했다.

WEP 내부 구조의 취약점: 첫째, 키스트림의 재사용 문제점이다. 24 비트의 초기화 벡터는 한 패킷 당 2^{24} 개의 키 중에 하나를 선택하여 전송한다면 초당 11M 비트를 전송하는 802.11b 무선 AP에서 5 시간 이내에 초기화 벡터가 재사용된다. 이것은 알고리즘의 약점이 아니라 WEP에서 알고리즘을 사용하는 방법의 문제점 때문에 발생한다. 둘째, 스트림 방식의 RC4 를 사용하기 때문에 발생하는 취약점이다. 스트림 암호는 입력이 같을 경우 출력이 같다. 한 개의 평문을 추정할 수 있는 경우 두 번째 암호문은 쉽게 해독될 수 있다. 셋째, 초기화 벡터가 전송되는 방식의 취약점이다. 시드값 중에서 초기화 벡터와 비밀키의 인덱스 값이 평문으로 전송된다. 넷째, 802.11 의 Shared-Key 인증 방식의 취약점이 있다. 전송되는 데이터를 수집해서 비밀키를 쉽게 해독할 수 있다.

무결성 알고리즘의 취약점: 비밀키를 사용하지 않는 CRC-32 의 선형적 특징을 이용하면 공격자는 암호화된 데이터를 수정할 수 있다. CRC도 수정할 수 있기 때문에 단말기나 AP는 공격을 인지할 수 없다. 또한, WEP의 무결성 알고리즘은 모든 정보를 보호하지 않는다. 이것은 중요한 정보를 노출한다.

5. WEP 비밀키 공격 기법

5.1 전수 조사 공격 (Brute Force Attack)

WEP에 대해 오프라인 전수 공격을 하는 것은 다음과 같다. 몇 개의 패킷을 수집한 후 가능한 모든 키를 이용해 그 패킷을 복호화 해보는 방법이다. 그리고 복호화한 패킷의 CRC를 계산해서 원본과 비교한다. 만약 그 둘이 일치하면 그 키는 올바른 키일 가능성이 매우 높다. 일반적으로 이 확인 작업은 적어도 2 개의 패킷에 대해 하는 것이 좋다. 왜냐하면 서로 다른 두 키로 복호화한 메시지의 CRC는 같은 경우가 있기 때문이다.

Tim Newsham은 사전 공유 키 기반의 알고리즘의 약점을 공격하는 효율적 공격 기법을 만들었다. 그가 만든 방법을 이용하면 40 비트의 키 공간을 21 비트까지 줄일 수 있다.

5.2 키스트림 재사용 공격

WEP이 가진 또 하나의 잠재적 문제점 중 하나는 키스트림을 재사용하는 것이다. 만약, 초기화 벡터가 무작위로 선택된다고 가정하면, 통계적으로 약 5,000 개의 패킷을 사용할 때마다 키스트림이 재사용된다.[2] 초기화 벡터의 무작위 선택이 재사용 확률을 높이는 것이다.

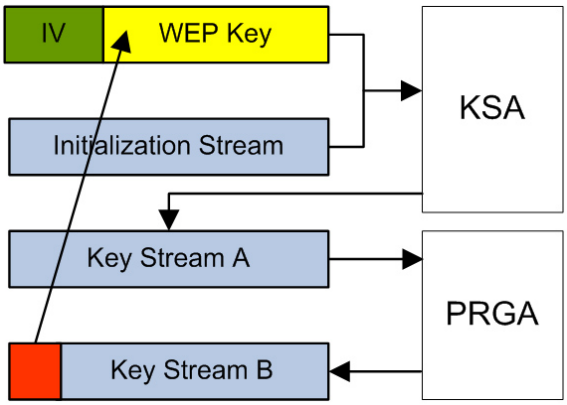
초기화 벡터 재사용이 일어날 경우 비밀 키와 재사용된 초기화 벡터에 의해 생성된 키스트림은 이전 것과 동일하다. WEP에서 평문은 인터넷 패킷이기 때문에 미리 추측할 수 있는 구조로 되어 있다. 만약 두 평문 중 하나를 알았다면 나머지 하나의 평문을 쉽게 알 수 있다.

5.3 재전송 공격 (Replay Attack)

WEP에서 취약한 무결성 보호로부터 재전송 공격이 가능하다. 재전송 공격 방법은 우선 무선랜 상으로 전송된 802.11 패킷들을 수집한 후 AP가 필요한 정보를 포함한 패킷으로 수정하여 재전송한다.

5.4 FMS 공격 (Fluhrer, Mantin, Shamir Attack)

FMS 공격은 WEP 공격에 가장 중요한 방법이다. 본래 이 공격은 RC4 를 목적으로 제안되었다. 이 공격 방법에서 RC4 의 KSA(Key Scheduling Algorithm)와 PRGA(Pseudo Random Generation Algorithm)의 약점과



(그림 2) RC4 알고리즘과 FMS 공격

더불어 WEP에서의 초기화 벡터의 사용법의 약점을 이용한다.

초기화 벡터 중에는 키스트림의 첫 번째 바이트에 비밀키에 대한 정보를 노출시키는 약한 초기화 벡터가 있다. 패킷을 암호화할 때 초기화 벡터는 계속 바뀌지만 비밀키는 고정값이기 때문에 약한 초기화 벡터를 사용하는 충분한 패킷을 수집했고 키스트림의 첫 번째 바이트를 알고 있다면 통계적으로 역추적하는 방법을 사용해서 비밀키를 알아낼 수 있다.

약한 초기화 벡터의 구조와 증명은 [2]와 [8]에 설명되어 있다. 802.11 패킷의 최초 8 바이트는 논리적 연결 제어부와 서브 네트워크 접근 프로토콜 헤더로 구성되고 거의 모든 경우에 고정된 값이다. 이것을 이용하면 암호 패킷에 적용된 키스트림의 처음 부분을 알아낼 수 있다.

위 과정으로 추정한 값이 올바른 키일 확률은 5%이다. [2] 이 작업을 초기화 벡터를 변화시키며 여러 번 수행하면 올바른 키 바이트 값을 얻을 수 있다. 약 60 개의 IV를 시도하면 올바른 키를 얻을 확률은 50%이상이다. 키 바이트를 얻어낸 후에 순차적으로 반복하면 그 다음 키 바이트를 얻어낼 수 있고 결과적으로 전체 키를 얻어낼 수 있다.

5.5 KoreK 공격 (KoreK Attack)

KoreK 공격은 Fluhrer의 FMS 공격의 확장된 공격이다. KoreK 공격은 모든 패킷을 대상으로 하고, FMS 공격을 포함한 17 가지 공격을 정의하고 있다. 각각의 공격은 초기 조건과 증명, 정규식으로 구성된다.

Korek 공격의 기법은 세 가지로 구분될 수 있다. 첫 번째 그룹은 PRGA의 출력 스트림의 첫 번째 바이트로부터 키를 복구하는 방법에 대해서 정의한다. FMS 공격의 알고리즘이 첫 번째 그룹에 속한다. 두 번째 그룹은 출력 스트림의 첫 번째 바이트 이후의 정보를 활용해 키를 복구하는 방법을 정의한다. 세 번째 그룹은 키 탐색 범위를 줄이는 방법과 올바른 비밀키를 선택할 수 있는 조건에 대해서 정의한다.

5.6 단편화 공격 (Fragmentation Attack)

단편화 공격은 WEP로 보호되는 네트워크가 인터넷과 연결되어 있을 때만 사용할 수 있다. 공격의 기본 아이디어는 데이터 패킷을 수집해서 IP헤더 정보를 획득하고, 패킷을 변경하여 필요한 정보를 포함시킨 후에, 분할해서 전송하고 암호화된 텍스트의 복호화를 AP에게 맡긴 후 자신의 컴퓨터로 평문으로 전송되게 하는 것이다. 이러한 공격이 가능한 이유는 이미 알려진 평문이 포함된 패킷에서 획득한 키스트림을 바탕으로 WEP 무결성 알고리즘의 취약점을 이용해 패킷을 변조하는 것이 가능하기 때문이다.

6. 구현 및 실험

우리는 위에서 언급한 비밀키 공격 기법을 이용해서 효율적인 비밀키 공격 기법을 제안한다. 제안한 공격 기법을 실제 구현한 후 실험을 실시한다.

기존에 개발된 프로그램으로 AirSnort와 AirCrack, WebLab이 있다. AirSnort는 FMS 공격을 사용하는 프로그램이고, AirCrack과 WebLab은 KoreK 공격을 바탕으로 설계되었다. 우리가 설계한 프로그램은 AirCrack을 바탕으로 기존의 알고리즘과 새로운 알고리즘을 통합한 형태이다.

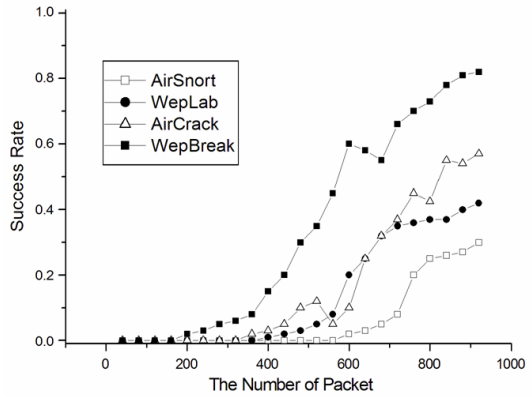
공격은 다음의 순서로 진행된다.

① AP가 주기적으로 전송하는 Beacon 메시지를 이용해 공격에 필요한 정보를 수집한다.
② 수집된 정보를 바탕으로 AP의 인증 및 암호 방식을 파악한다.
③ 이미 알고 있는 패킷의 정보를 사용해서 비밀키의 처음 8 바이트를 해독한다.
④ IP 데이터를 포함한 패킷의 정보를 변경해서 필요한 크기로 단편화해서 전송한다.
⑤ 단편화 공격으로 목적한 컴퓨터에 패킷이 전송된 경우, 해당 AP는 외부 인터넷과 연결되어 있다. 이 경우, 재전송 공격을 이용해 비밀키를 복호화할 수 있다.
⑥ 단편화 공격이 실패한 경우 ARP 요청 메시지를 재전송하는 방법으로 AP의 암호화 데이터 생성을 유도한다. 충분한 패킷을 수집한다.
⑦ Erik Tews가 제안한 통계적 방법을 사용한다. 이 방법은 KoreK 공격을 바탕으로 가능성이 높은 키에 가중치를 부여해서 바이트 기준으로 키를 정렬한다.
⑧ 정렬된 키를 입력으로 Tim newsham의 최적화 알고리즘을 적용해 유효한 키를 검색한다.
⑨ 검색된 키로 제한된 전수 공격을 실시한다.
⑩ 계산된 키는 여러 패킷에 대한 CRC계산을 통해서 검증한다.

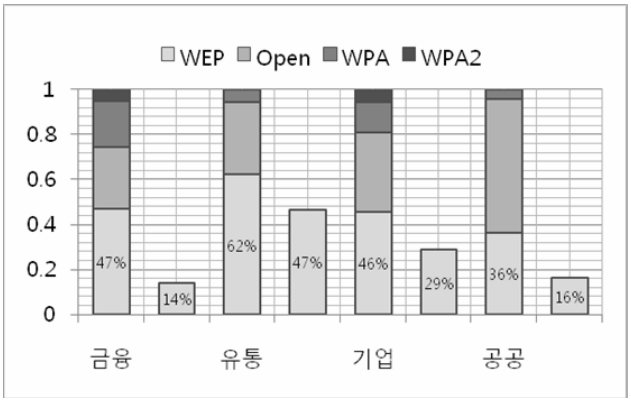
AP는 두 가지 모델을 사용했고, 사용한 단말은 3Com 무선랜카드와 인텔 모바일 칩셋의 노트북을 사용했다. 일반적인 환경에서의 실험을 목적으로 했기 때문에 외장 안테나를 사용하지 않았고 무선랜카드에 포함된 내장 안테나를 이용했다.

실험은 성공률 측정 실험과 실제 환경에서의 알고리즘 적용 실험으로 구분해서 진행한다.

성공률 측정 실험은 직접 AP를 설치하고 임의로 설정한 비밀키를 프로그램을 사용해서 알아내는 방법으로 진행한다. 지정된 시간 내에 키를 해독하고 검증된 키의 경우 성공으로 기록했다.



(그림 3) 알고리즘 별 성공률



(그림 4) 분야별 알고리즘 비율과 공격성공률

실제 환경에서의 적용 실험은 기존의 설치되어 사용되는 AP에 대해서 비밀키를 알아내는 방법으로 진행했다. 공격의 성공여부는 지정된 시간 내에 키를 알아내 후 AP로의 접속 여부로 판단했다.

알고리즘 별 성공률 측정 실험의 결과는 위의 그래프와 같다. 128 비트의 WEP를 기준으로 실험한 결과이다. 64 비트의 경우도 비슷한 분포를 보인다. WepLab과 AirCrack은 패킷의 증가에 따라 비슷한 성공률 변화를 보여준다. 우리가 제시한 알고리즘은 단편화 공격이 성공한 경우는 성공한 경우로 분류하고, 실패한 경우는 일반 알고리즘을 적용해서 성공한 경우와 실패한 경우를 구분했다. 200 만개의 패킷부터 성공률 변화를 보이다가 550 만개 이후로는 50%이상의 성공률을 보인다. 제한시간을 가정한 실험에서 적은 수의 패킷으로 키가 해독된다는 것을 확인할 수 있다.

실제 환경에서의 알고리즘 적용 실험 결과는 아래 그래프와 같다. 각각의 부분은 알고리즘의 분포를 의미하고, 각 항목별 두 분째 그래프는 WEP에 대한 공격 성공률을 표현한다.

유동인구가 많고 무선랜의 사용이 예상되는 지역을 선정하고, 예상지역을 금융, 유통, 기업, 공공 분야로 분류했다. 각각의 분야별로 AP가 전파하는 Beacon 메시지를 이용해서 네트워크의 정보를 조사했다.

수집한 정보를 바탕으로 보안 알고리즘의 비율을 조사한 결과 모두 1873개의 AP중에서 37%(699)인 곳이 공개된 시스템을 사용하고, 50%(936)인 곳이 WEP를 사용했다. 보안성이 강화된 WPA의 경우는 10%(193)와 2%(45)였다. 주로 WEP를 사용하는 것을 확인할 수 있다.

WEP의 사용이 확인된 AP에 대해서 제안된 알고리즘을 이용한 공격을 시도해서 그 성공률을 기록했다. 이 경우 64비트와 128비트 WEP의 합산이다. 금융의 경우 대부분 128비트 WEP를 사용해서 성공률이 매우 낮다. 반면에 유통의 경우는 WEP의 확인된 모든 경우 64비트를 쓰고 있었고 따라서 성공률이 매우 높다.

WEP로 보호된 네트워크는 높은 확률로 공격이 가능하다. 위 실험에서는 일반적인 장비를 사용하고, 제한 시간을 두었기 때문에 실패하는 경우가 발생한다. 키 해독을 위한 계획적인 공격에 대해서 WEP로 보호된 네트워크는 더 이상 안전하지 않다. 일반 유저에게 공개하기 위한 목적이 아니라 비밀통신을 목적으로 하는 네트워크에서 보안을 위해 WEP를 사용하는 것은 매우 위험하다. 전송되는 데이터의 보호를 위해서는 다른 방법을 사용해야만 한다.

7. 결론

본 논문에서 WEP의 취약점을 기반으로 한 공격 알고리즘을 제안했다. 이 알고리즘은 동적인 알고리즘과 정적인 알고리즘을 병행해서 사용한다. 알고리즘을 적용한 실험 결과 WEP로 보호되는 네트워크는 짧은 시간 내에 비밀 정보가 노출된다. 일반적인 환경 조건에서 실행된 실험은 WEP의 위험성을 분명하게 보여준다. AP는 다른 네트워크로의 관문 역할을 수행하기 때문에, WEP 공을 통한 AP로의 접속은 차후 다른 공격의 발판이 될 수 있다. 이러한 이유로 보안을 목적으로 한 네트워크에서 WEP를 사용하는 것은 위험하다. WEP는 완전한 보안을 제공하지 않는다.

참고문헌

[1] David Wagner, “Intercepting Mobile Communications - The Insecurity of 802.11”, In MOBICOM July 2001

[2] Scott R. Fluhrer, “Weaknesses in the Key Scheduling Algorithm of RC4”, 2001

[3] Rafik Chaabouni, “Break WEP Faster with Statistical Analysis”, Semester Project, June 2006

[4] Andrea Bittau, “The Final Nail in WEP’s Coffin”, IEEE Security and Privacy, May 2006

[5] Erik Tews, “Breaking 104 bit WEP in less than 60 seconds”, Apr 2007

[6] W. A. Arbaugh, “An Inductive Chosen Plaintext Attack.Against WEP and WEP2 ” IEEE 802.11 Working. Group, Task Group I (Security), 2002.

[7] Adam Stubblefield, “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”, Feb 2001.

[8] Andrew Roos, “A Class of Weak Keys in the RC4 Stream Cipher” - Preliminary Draft, Sep 1995

[9] R. L. Rivest, “The RC4 Encryption Algorithm.” RSA Data Security, Inc., mar. 12, 1992 (Proprietary)

[10] IEEE Computer Society. ANSI/IEEE Standard 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.