박미애 김용희
김창범 이옥연
Kookmin University

무선랜의 데이터 프라이버시 알고리즘 구조 분석

AM-1

WLAN의 매체 특성상 AP beacon 영역 내의 모든 STA들은 다른 STA의 송수신 데이터 내용에 접근할 수 있다. 따라서 상호 또는 그룹 간의 데이터 프라이버시와 상호인증 서비스는 무선 랜의 중요한 이슈중의 하나이다.

무선랜을 통한 네트워크 접속 보안으로는 사용자와 AP 사이의 무선 접속 구간 보안과 AP와 AS사이의 유선 구간 보안으로 정의되며, 상대적으로 취약한 무선 구간 보안이 초점이 된다. 현재 무선 구간 보안에는 WEP이 사용된다. 그러나 WEP 방식은 WEP 키와 IV 크기가 작고, 노출된 공유키를 사용하며, 암호 알고리즘(RC4)와 무결성 알고리즘(CRC-32)이 근본적으로 취약하다. 이러한 문제에 대한 해결 방법으로 IEEE 802.11i는 두 가지 접근 방식을 채택하였다. 하나는 WEP의 보안 문제점을 소프트웨어적으로 개선한 TKIP이고 다른 하나는 기존의 WEP과는 하드웨어적으로 상이한 AES을 기반으로 한 CCMP이다.

이 논문에서는 각 알고리즘에 대한 키의 흐름 및 그 안전성을 분석하였다. 이러한 방법을 통해 WEP 구조의 보안상의 취약점을 확인하고, TKIP이 WEP을 대체할 수 있을 만큼의 안전성을 갖는지를 검증한다. 또한 고려될 수 있는 공격 모델을 제시하고, 이에 대하여 알고리즘에 부가적으로 요구되는 보완점에 대해 논한다.

김학준 신현구
문일현 이종근
이옥연
Kookmin University

무선랜 보안 알고리즘의 난수성 분석

AM-2

PRF(Pseudo Random Function)에 대한 랜덤성 검증은 pre-computation 공격에 대해 알고리즘이 특별한 통계적 약점이 없이 적절하게 개발되었는지를 평가할 수 있다.

이 논문에서는 NIST에서 실시한 AES 후보 알고리즘 랜덤성 평가 기준을 적용하여 IEEE의 802.11i Draft에서 인증자와 요청자가 비밀키(PTK, GTK)를 생성하는데 사용되는 PRF의 랜덤성을 검증하였다.

랜덤성 테스트를 위해 표본 수는 300개, 표본 길이는 2^{20}(= 1,048,576)으로 검정 표본을 생성하고, 유의 수준은 0.01로 선택하였다. 랜덤성 검증 방법으로는 NIST의 16가지 통계 테스트를 사용하였다.