AES 암호 방식에서의 암호 키 길이 변화에 따른 넌어드레스 장비의 성능 측정 및 비교

이원준, 최훈
충남대학교 컴퓨터공학과
e-mail: wonjnlee@gmail.com, hc@cnu.ac.kr

Performance comparison by key length of AES encryption using Non-Addressable Data Protection Devices

Wonjoon Lee, Hoon Choi
Dept. of Computer Science and Engineering, Chungnam National University

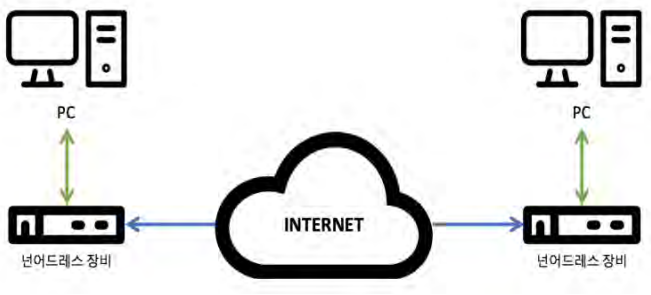
요 약

넌어드레스(Non-Addressable) 장비는 IP 주소를 포함한 기타 어느 계정을 갖지 않는 통신 보안 장비로서, 해킹을 포함한 허가되지 않은 공격들로부터 원천적으로 단말을 보안할 수 있다. 본 논문에서는 넌어드레스 장비에서 AES 방식으로 데이터를 암/복호화 시 성능을 향상시키기 위한 방법을 제시한다. AES-128, 192, 256 에서의 암/복호화 시간, CPU 사용량, 메모리 사용량, 실제 데이터의 전송 속도를 비교하여 최선의 설정 방법을 도출한다.

1. 서론

최근 인터넷을 포함한 IT 환경의 발달은 인간의 생활에 편리함과 신속함을 포함한 공간의 한계가 없는 새로운 생태계를 만들고 있지만, 보안이라는 해결해야 할 문제점을 안고 있다. 인터넷을 통하여 손쉽게 다양한 정보의 접근이 가능해졌지만, 이로 인하여 개인 또는 기업 정보의 유출이 빈번하게 발생하고 있다. 여러 국가 및 기업에서는 정보의 유출을 막기 위하여 많은 예산을 보안 환경 구축에 사용하고 있다[1][2][3].

본 논문에서 이용하는 넌어드레스 장비는 IP 주소를 포함한 어느 계정도 장비에 존재하지 않는 통신 보안 장비로서, PC 나 VoIP 전화기와 같은 인터넷을 사용하는 단말과 연결되어 허가된 상대 넌어드레스 장비로부터 수신된 데이터만 단말로 전달한다[4][5][6].



(그림 1) 넌어드레스 장비 동작 예시

두 넌어드레스 장비가 서로 허가된 장비임을 확인하면, 단말기에서 송신된 데이터는 연결된 넌어드레스 장비에서 허가된 장비끼리 서로 약속된 암호키로 암호화되어 네트워크에 전송한다. 넌어드레스 장비는 네트워크로부터 수신한 데이터를 서로 약속된 암호키로 복호화하고 연결된 단말기로 복호화된 데이터를 전달한다.

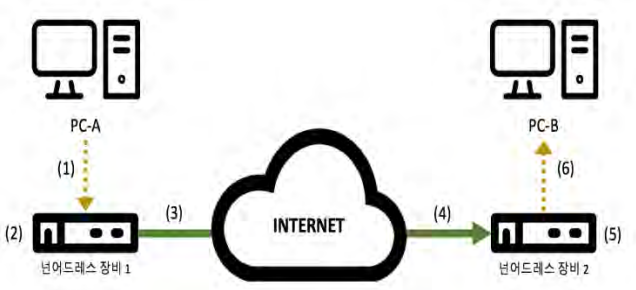
본 논문은 넌어드레스 장비에서 AES 알고리즘을 사용하여 데이터 암/복호화를 진행할 경우, 암호 키 길이의 변화에 따른 장비의 성능을 측정하고, 이를 통한 최적의 설정 방법을 도출한다. 측정 대상으로는 암복호화에 소요되는 시간, CPU 사용량, 메모리 사용량, 데이터 전송 시 발생하는 속도 및 대역폭을 선정하였다.

저자들이 파악한 바로는 본 논문이 넌어드레스 장비를 대상으로 성능을 분석한 첫 연구 시도이다.

2. 배경 기술

2.1. 넌어드레스 장비를 이용한 통신 과정

넌어드레스 장비는 PC, VoIP 등 인터넷과 연결되어 사용하는 단말의 앞 단에 연결되어 인터넷망과 단말 사이에 위치한다.



(그림 2) 넌어드레스 장비 내 암복호화 순서도

단말에서 인터넷망으로 전송하는 데이터(1)를 허가된 넌어드레스 장비에서만 복호화될 수 있도록 재가공(2)한 후 인터넷망으로 전달(3)한다. 인터넷망으로부터 수신된 데이터(4)는 먼저 넌어드레스 장비 내에서 허가된 넌어드레스 장비로부터 전달된 데이터인지 여부를 확인하고, 정상 데이터인 경우에만 복호화를 진행(5)하여 정상적으로 복호화 된 데이터를 단말로 전달(6)한다.

넌어드레스 장비와 연결된 단말로부터 송신된 데이터의 암호화(2) 및 허가된 넌어드레스 장비로부터 재가공되어 인터넷 망을 통해 수신된 데이터의 복호화(5)에 사용되는 암호 키(A)는 1.패킷의 정보를 통해 생성되어 패킷마다 매번 변동되어 고정되지 않은 값을 사용하도록 설계된 암호키(B)와, 2. 키 교환 작업을 통해 통신이 구성된 세션마다 다르게 생성되는 별도의 비밀키(C)를 조합(A=B+C)하여 생성된다[6][7][8][9].

암호에 사용되는 알고리즘은 사용자의 기호에 따른 다양한 적용이 가능하나, 기본적으로 AES 알고리즘을 적용하고 있다. 본 논문은 AES 알고리즘을 사용하여 실험을 진행한다.

2.2. AES 알고리즘

국가 표준으로 사용되었던 DES(Data Encryption Standard)의 취약점을 보안하기 위해 고안된 암호 알고리즘이다[10].

AES(Advanced Encryption Standard) 암호 알고리즘은 기존의 DES 암호 알고리즘의 취약점이었던 짧은 키의 길이 문제를 해결하였다. 암호 블록 크기는 128bit 이다. 또한 알고리즘의 변경 없이도 128bit 뿐만 아니라 192bit, 256bit 블록 크기로 확장이 가능하다.

3. 실험

3.1. 실험 목적

AES 알고리즘은 128bit, 192bit, 256bit 의 다양한 암호키 길이를 적용하여 데이터를 암복호화할 수 있는 장점을 갖는다. 암호키의 길이가 증가할수록 데이터의 보안 강도는 더욱 견고해지지만, 암호키 생성 및 암복호화 동작에 발생하는 시스템의 부하가 증가하여 데이터 전송 속도를 포함한 전체적인 성능이 저하될 수 있다.

그러므로 본 논문은 넌어드레스 장비에서 AES 알고리즘을 이용한 데이터 암복호화를 진행할 때, 암호키 길이 변화에 따른 여러가지 성능 측정 결과를 이용하여, 최적의 성능을 얻을 수 있는 결론을 도출함에 있다.

3.2. 실험 환경

본 연구의 실험에는 넌어드레스 장비의 한 종류인 Ghost[4][5]를 사용하였으며, 넌어드레스 장비를 이용한 실험 환경의 구성은 다음과 같다.

(그림 3) 실험 환경 구성도

<표 1> Ghost 환경

CPU	AMD Celeron 800MHz
Memory	128mb
운영체제	Linux Fedora
네트워크 속도	10/100Mbps

<표 2> 단말 노트북 환경

CPU	2.6 GHz Intel Core i5
Memory	8 GB 1600 MHz DDR3
운영체제	macOS Sierra

두 단말 노트북 사이의 데이터 송수신을 위하여 iperf 프로그램을 사용하였다. iperf는 비영리적 프로그램으로 운영체제의 종류에 관계없이 간편하게 대역폭, 전송 량을 포함한 네트워크 상태를 측정할 수 있다[11].

3.3. 시나리오

본 논문에서 사용할 실험 지표는 다음과 같다.

- 암호 키 생성에 소요되는 시간
- 데이터 암복호화에 소요되는 시간
- 넌어드레스 장비의 최대 CPU 사용률
- 암복호화 프로세스의 최대 CPU 사용률
- 암복호화 프로세스의 메모리 사용량
- 데이터 송수신에 발생하는 대역폭

암호화 작업은 CPU 에 많은 부하를 주기 때문에,

데이터를 지속적으로 보내게 되면 암호키 길이에 따른 CPU 사용률 차이를 명확하게 보이는 것이 어렵다. 그래서 뚜렷한 차이를 보일 수 있도록 하기 위해, 데이터를 1 초만 보내는 경우의 순간 CPU 사용률과 10 초동안 지속적으로 보내는 경우의 최대 CPU 사용률을 측정해 비교하였다.

3.4. 실험 결과

3.4.1. 평균 CPU 사용률

<표 3> 데이터 송수신 시 넌어드레스 장비 CPU 평균 사용률

	1 초	10 초
AES 128	21.495%	68.82%
AES 192	23.64%	69.375%
AES 256	23.8%	82.535%

<표 4> 암복호화 프로그램 실행 시 CPU 평균 사용률

	1 초	10 초
AES 128	30.77%	98.675%
AES 192	33.22%	99.695%
AES 256	38.345%	99.9%

넌어드레스 장비에서 1 초 간 데이터를 송수신할 경우 CPU 사용률와 넌 어드레스 장비에서 암복호화 프로그램을 실행시킬 때 CPU 사용률 모두 키 길이의 증가에 비해 근소한 차이로 CPU 사용률이 증가하였다. 반면에 10 초간 데이터를 송수신할 경우 넌어드레스 장비는 AES 256 에서 CPU 사용률이 크게 증가하였다. 암복호화 프로그램의 경우 키 길이에 상관없이 약 99% 이상의 CPU 를 사용하였다.

3.4.2. 평균 메모리 사용량

<표 5> 10 초간 데이터 송수신 시 넌어드레스 장비 평균 메모리 사용량

AES 128	78985 KiB
AES 192	89119.9 KiB
AES 256	89234.3 KiB

키의 길이가 증가할수록 넌어드레스 장비에서 사용하는 평균 메모리 사용량이 증가하였다. 이 이유는 키 길이의 증가로 인한 암복호화의 계산이 복잡해짐에 따라 사용하는 메모리의 양이 증가하였기 때문이다.

3.4.3. 소요 시간 측정

<표 6> 10 초간 데이터 송수신 시 패킷 별 암호 키 생성 평균 소요 시간

AES 128	0.000017 sec
AES 192	0.000018 sec
AES 256	0.000019 sec

<표 7> 10 초간 데이터 송수신 시 패킷 별 암호화 평균 소요 시간

AES 128	0.0003707 sec
AES 192	0.0004339 sec
AES 256	0.0004852 sec

<표 8> 10 초간 데이터 송수신 시 패킷 별 복호 키 생성 평균 소요 시간

AES 128	0.0000164 sec
AES 192	0.000017 sec
AES 256	0.0000182 sec

<표 9> 10 초간 데이터 송수신 시 패킷 별 복호화 평균 소요 시간

AES 128	0.0000107 sec
AES 192	0.0000114 sec
AES 256	0.0000132 sec

예상대로 키의 길이가 증가할수록 암호키 및 복호키 생성시간과 암호화 및 복호화 시간 모두 증가하였다. 그러나 암복호 키 생성 시간은 큰 차이가 없었으며, 암호화 시간이 복호화 시간보다 더 많이 소요되었다.

3.4.4. 평균 송신자 데이터 전송량 및 대역폭

<표 10> 10 초간 데이터 송수신 시 송신자 측 평균 데이터 전송량

AES 128	21.3 Mbytes
AES 192	19.785 Mbytes
AES 256	18.505 Mbytes

<표 11> 10 초간 데이터 송수신 시 수신자 측 평균 데이터 전송량

AES 128	21.2 Mbytes
AES 192	19.625 Mbytes
AES 256	18.4 Mbytes

<표 12> 10 초간 데이터 송수신 시 송신자 측 평균 대역폭

AES 128	17.895 Mbits/sec
AES 192	16.6 Mbits/sec
AES 256	15.505 Mbits/sec

<표 13> 10 초간 데이터 송수신 시 수신자 측 평균 대역폭

AES 128	17.8 Mbits/sec
AES 192	16.49 Mbits/sec
AES 256	15.4 Mbits/sec

키의 길이가 증가할수록 암복호화에 소요되는 시간이 증가하면서 초당 송수신할 수 있는 데이터의 양이 감소하였고, 이에 송신자 및 수신자 측 대역폭 모두 감소하였다.

10 초 이상 지속적으로 데이터를 송수신하면 키 길이가 증가할수록 소요 시간이 비례하여 증가하였지만, 최저 길이인 128bits 와 최장 길이인 256bits 의 암복호키 생성 및 암복호화 시간차가 매우 근소하였다. 그리고 키 길이가 증가할수록 평균 데이터 전송량 및 대역폭이 감소하였지만, 그 차이 또한 크지 않았다.

넌어드레스 장비의 10 초간 CPU 사용률 및 메모리 사용량의 경우 가시적인 증가율을 확인할 수 있었다. 하지만 실험에 사용한 하드웨어의 장비 성능에 비교할 때, 하드웨어 성능은 충분히 증가할 수 있기 때문에 키 길이에 따른 넌어드레스 장비의 성능 차이는 충분히 좁혀질 수 있을 것이다.

4. 결론

본 연구에서는 넌어드레스 장비에서 AES 알고리즘을 사용할 경우 최적의 키 길이를 적용하기 위해, 넌어드레스 장비를 사용하여 송수신하는 데이터를 128, 192, 256bit 키 길이를 갖는 AES 알고리즘을 이용하여 암복호화하고, 각 경우에 대한 시스템 성능 및 암복호화 소요 시간을 측정하였다.

키 길이가 증가할수록 당연히 CPU 사용률 및 메모리 사용량, 암복호키 및 암복호화 소요 시간은 증가하였으며, 데이터 전송량 및 대역폭은 감소하였다. 암복호키 및 암복호화 소요 시간의 경우, 키 길이가 늘어나도 측정값은 차이가 미비하였다. CPU 사용률 및 메모리 사용량은 암호키가 길어질수록 크게 증가하지만, 하드웨어 성능이 증가함에 따라 차이를 충분히 좁힐 수 있을 것이다.

결론적으로 128bit 보다는 192bit 암호키를 사용하는 경우 보안성은 크게 강화하면서 성능에 큰 영향을 주지 않을 것이다. 고성능의 하드웨어를 사용할 경우 256bit 키를 사용하여도 장비의 성능에 큰 영향을 주지 않을 것으로 판단한다.

향후 연구로는 고성능 하드웨어에서 동일한 실험을 진행하고, 성능 증가에 따른 적절한 하드웨어 구성을 제안할 것이다. 또한 내부 암복호화 알고리즘 개선을 통한 소요 시간 감소 방안을 제안할 것이다.

감사문

최훈은 2017 년도 한국연구재단 이공학 개인기초연구사업(NRF-2017R1D1A1B03029262)의 지원을 받아 수행하였음

참고문헌

[1] 김유진, 이누리, 신성은, 손승연, 정다영, “사물인터넷(IoT) IP 의 노출과 위협에 대한 연구”, The Journal of the Convergence on Culture Technology (JCCT), Vol.2 No.4, pp. 77-82, 2015.

[2] 조희영, “이제 보안은 선택이 아닌 필수”, 매일경제, http://news.mk.co.kr/newsRead.php?year=2017&no=530046, 2017.

[3] 신혜원, 지성우, “사물인터넷(IoT) 환경에서의 개인정보보호에 관한 규범적 고찰”, 법과 정책 22 권 2 호, pp. 427-454 , 2016.

[4] 김아연, “[인터뷰]주대준 한국사이버보안컨버젼스학회장, 보안 혁명 ‘GHOST’를 말하다”, Weekly Today, http://m.weeklytoday.com/news/articleView.html?idxno=36219#0648, 2015.

[5] Ghost Waltzer, http://www.ghostwaltzer.com, accessed on Aug. 2017.

[6] 이광원, “넌어드레스 네트워크 장비를 이용한 통신 보안 시스템 및 방법 (Communication security method and system using a non-address network equipment)”, 국내 특허, 출원번호: 10-2016-0157227, 2016.

[7] 이광원, “데이터 암호화 및 복호화 시스템 및 방법 (Data encryption and decryption system and method thereby)”, PCT, 출원번호: PCT/KR2016/013600, 2016.

[8] 이광원, “데이터 암호화 및 복호화 시스템 및 방법 (Data encryption and decryption system and method thereby)”, PCT, 출원번호: PCT/KR2016/013609, 2016.

[9]이광원, “데이터 암호화 및 복호화 시스템 및 방법 (Data encryption and decryption system and method thereby)”, PCT, 출원번호: PCT/KR2016/013613, 2016.

[10] Wikipedia, “ Advanced Encryption Standard,” https://en.wikipedia.org/wiki/Advanced_Encryption_Standard, access on Aug. 2017.

[11] Wikipedia. “Iperf,” https://en.wikipedia.org/wiki/Iperf, access on Aug. 2017.