분산 네트워크 환경에서 2-MAC 인증 패킷을 이용한 공격자 추적기법

서대희, 이임영
순천향대학교 정보기술공학부

A Study on Attacker trace techniques applying 2-MAC authentication packet in Distribution Network

Dae-Hee Seo, Im-Yeong Lee
Division of Information Technology Engineering. SoonChunHyang University

요약

최근 인터넷을 대상으로 한 사이버 공격의 공격 경향은 분산 환경에서 다수 공격자의 대규모 분산 서비스 거부 공격(DoS)의 출현 및 해외 해커들의 국내 전산망을 우회 루트로 활용한 사례의 증가 등 고도화된 불법 행위가 점차 범죄의 강력한 수단으로 이용되는 추세에 있다.

본 논문은 기존 네트워크에서 해당 네트워크의 침입자의 트래픽 차단 방법의 취약점을 보완하여 2-MAC 인증 패킷을 이용한 효율적인 공격자 추적기법을 제안하였다. 제안된 방식은 기존 시스템에서의 NIC(Network Interface Card)의 물리적 주소인 MAC(Media Access Control)과 메시지 인증 코드(MAC:Message Authentication Code)를 이용한 방식을 제안하였다.

1. 서 론

인터넷의 이용이 확산되면서 이를 기반으로 한 전자상거래의 증가와 전자 정부의 실현에 따라 주요한 사회기반 시설(SOC, Social Overhead Capital)과 대규모 생산 시설등의 운영 관리가 정보시스템을 이용하여 수행되고 있다. 그러나 고도화된 정보 사회에서는 국가의 많은 기능들이 정보 통신 시스템에 연동되어 이를 관리하고 유지하는데 어렵기 때문에 보안 취약점을 나타내고 있다. 특히 현재의 사이버 공격에 대한 여러 종류의 대응 방안에 대한 모색은 국가적 차원에서 반드시 필요한 연구로 대두되고 있는 실정이다[1][2].

따라서 본 논문에서는 기존의 네트워크 공격자 추적 기법에 대한 내용들을 분석하고 보다 효율적인 공격자 기법을 제안하고자 한다. 제안된 방식은 최초 접속 라우터로부터의 공격 차단을 통해 공격자의 네트워크 연결 자체를 차단함으로써 향후 예측되는 다양한 공격 방법으로부터 내부 네트워크의 안전성을 유지할 수 있다.

2. 기존 네트워크 공격자 추적 방법

다음은 기존의 네트워크 공격자 추적 기법과 상용화 제품에 대해 분석한다.

① 사용화된 공격자 추적 제품 분석

현재 개발된 공격자 추적 제품의 경우 다음과 같은 취약점을 가지고 있다[2].

- 상호 운용성이 결핍되어 있다.
- 수동적인 보안 시스템 재구성으로 인한 대응 시간 지연으로 능동적인 대응이 어렵다.
- 중간 공유지역의 보안성 부족으로 우회 공격의 가능성을 내포하고 있다.
- 새로운 공격 기술에 대한 대처 능력이 저하된다.

② IDIP(Intruder Detection and Isolation protocol)

IDIP는 네트워크 보안 요소들간의 협력작업을 포함하는 보안 기반 프로토콜로써 공격자의 실제 위치추적 메커니즘을 개발하는데 그 목적이 있다. 그러나 다음과 같은 취약점이 노출되고 있다[3][4].

- 모든 IDIP 노드에 패킷에 대한 로그를 남겨야 한다
- 모든 호스트와 백본 네트워크 라우터는 IDIP 기능을 수행해야 한다.
- 새로운 기능의 추가나 변경이 어렵다
- 보안 환경에 대한 유연성이 떨어지며, 확장

하기가 어렵다.

③ AN-IDR(Active Network Intrusion Detection and Response)

AN-IDR은 DARPA의 프로젝트로 1999년부터 수행된 침입자 대응 프로토콜이다. 이는 기존의 공격자 추적 기법이 제공하지 못하고 있는 이동성과 유연성, 확장성에 그 목표를 두고 연구가 진행중에 있다.[3~5]

그러나 AN-IDR의 경우 다음과 같은 기술적인 취약점을 분석할 수 있다.

- 모든 패킷에 대한 Connection Escort 정보를 저장해야 한다.
- 사용자의 프라이버시 정보로 생성되는 Connection Escort 패킷은 사용자의 프라이버시 정보를 침해할 수 있는 문제점을 발생시킨다.
- 지속적인 Connection Escort 정보 감시를 통한 적법성 논란이 지속되고 있다.
- 공격자의 추적 수준에 대한 Connection Escort 정보에 대한 설정 미비로 인한 추적의 한계성이 지적되고 있다.

3. 분산 네트워크에서 공격자 추적 기법의 요구사항

효율적인 네트워크 공격자 추적기법은 다음과 같은 요구사항을 만족해야 한다.

① 공격자의 공격 시간과는 무관해야 한다.

현재의 시스템은 공격자가 공격이 진행중일 경우에만 공격자의 추적이 가능하다는 한계점을 들 수 있다. 따라서 공격자의 공격이 이루어진 후에도 공격자에 대한 추적이 가능해야 한다.

② 내부 공격자의 공격에 대한 안전성

기존의 제안된 방식에서는 내부 공격자에 대한 안전성을 제공하지 않고 있다. 이는 네트워크 외부에 공격자가 있다는 가정으로 이루어지지만 실제적인 공격의 경우 내부 공격자가 신뢰되지 않는 사용자일 경우 내부 공격자에 대한 안전성을 제공할 수 있어야 한다.

③ 우회 공격에 대한 안전성

기존 방식에서는 공격자의 처음 공격에 대한 대응을 통해 공격자를 차단 및 추적하는 기능을 제공하고 있다. 그러나 공격자의 경우 다른 네트워크를 우회해 다시 해당 네트워크를 침해할 수 있는 우회 공격의 문제점에 대해 안전성을 제공하면서 이를 차단할 수 있어야 한다.

④ 범용적인 추적기법 제공

특정 일부 라우터에서만 제공되는 침입자 추적 기법은 이미 구축된 네트워크 환경에 적용하기엔 부적합하다. 따라서 기존의 네트워크에서도 네트워크 구성 요소를 새롭게 구성하지 않아도 제공할 수 있는 침입자 추적 기법이 요구된다.

4. 분산 네트워크에서 효율적인 공격자 추적기법 제안

본 논문에서는 모든 사용자가 초기 라우터에 접속시 전송되는 패킷과 더불어 2-MAC 인증 패킷을 통해 사용자의 인증을 수행한다. 수행된 패킷은 고유 순서번호를 가지고 최종 접속 라우터까지의 연결을 시도하게 된다.

4.1 가정사항

모든 노드의 라우터에는 2-MAC 인증 패킷의 경로 추적 프로그램을 내장하고 있으며, 본 논문에서 제안되는 2-MAC의 인증 패킷 구조는 그림 1과 같다.

"자동화 프로그램"	MAC 주소	인증 메시지 (MAC)	MAC 대응 IP	M, A, d	초기 RID, IID	TS

(그림 1) 2-MAC 인증 패킷 구조

- 자동화 프로그램 : 각 라우터에 저장된 침입 경로 추적 프로그램의 인스톨을 위한 명령어로써 침입이 탐지되었을 경우 해당 프로그램의 수행 정보
- MAC(Media Access Control) 주소 : NIC(Network Interface Card)의 고유한 물리 주소
- 인증 메시지(MAC : Message Authentication Code) : 사용자의 고유 개인 정보를 기반으로 한 사용자 MAC 정보로써 SHA와 MD5로 생성된 개인 정보
- M, A : 사용자의 초기 접속 메시지(M)을 기반으로 생성된 추적 인자(A)
- RID, UID : 공격자가 최초 접속된 라우터 ID와 초기 사용자 접속 ID
- TS(Time Stamp) : 초기 2-MAC 인증 패킷이 생성된 시간

4.2 시스템 계수

다음은 분산 환경에서 효율적인 공격자 추적을 위한 시스템 계수를 설명한다.

M : 공격자의 초기 접속 요청 메시지

g, n : 공개된 계수

r : 각각의 개체가 생성한 랜덤 수

H : 안전한 해쉬 함수

d_i : 신뢰된 기관에 등록되어 있는 각 개체의 고유 비밀 정보의 해쉬된 개인 정보 값(0 : 공격자, 1 : 라우터 A, 2: 라우터 B, 3: 라우터 C)

Sq : 2-MAC 인증 패킷의 순차번호

4.3 공격자 추적 프로토콜

2-MAC 인증 패킷을 이용해 효율적인 공격자 추적을 위한 프로토콜은 다음과 같이 이루어진다.

① 공격자는 초기 라우터 A의 연결을 위해 자신의 데이터 패킷과 함께 2-MAC 인증 패킷을 S와 함께 전송함으로써 접속을 요청한다.

$$S = M^{d_0} \bmod n$$

② 라우터 A는 2-MAC 인증 패킷에서 최초 접속 라우터의 ID와 접속로그 ID에서 라우터 A의 ID를 확인하고 해당 인증 메시지 코드(MAC)와 MAC 주소 그리고 대응 IP를 이용하여 로그 메시지를 생성한 후 다음을 계산한다.

$$S_{1=M}^{r_{A_1}} \bmod n$$

$$V_1 = g^{r_{A_2}} \bmod n$$

$$Z_1 = (M^{r_{A_1}} \times g^{r_{A_2}}) \bmod n$$

$$A_1 = H(Z_1^{d_1} \bmod n)$$

③ 공격자가 새로운 연결을 시도한 경우 초기 접속 라우터는 2-MAC 패킷의 랜덤한 고유번호(Sq)를 부여하고 새로운 연결 시도에 따른 패킷을 라우터 B에게 M, A_1, Sq_1, TS_1을 전송한다.

④ 라우터 B는 라우터 A와 동일한 방법으로 전송 패킷에 대한 랜덤한 고유번호(Sq_2)를 선택하여 다음을 계산한 뒤 더불어 라우터 C에 M, A_2, Sq_2, TS_2를 전송한다.

$$S_{2=M}^{r_{B_1}} \bmod n$$

$$V_2 = g^{r_{B_2}} \bmod n$$

$$Z_2 = (M^{r_{B_1}} \times g^{r_{B_2}}) \bmod n$$

$$A_2 = H(Z_2^{d_2} \bmod n)$$

⑤ 공격자는 라우터 C를 통해 침입 대상 네트워크에 침입을 시도할 경우 해당 라우터 C는 내부 보안 설정에 의해 침입 시도를 인지하고 이에 대한 경보 메시지와 자체 보안 설정에 따른 침입자 대응을 수행에 대한 메시지와 더불어 공격자가 라우터 C에 접속시 전송된 M, A_2, Sq_2, TS_2를 브로드캐스팅한다.

⑥ 라우터 B는 라우터 C의 공격자 대응 메시지와 M, A_2, Sq_2, TS_2를 수신한 후 이에 대응되는 M, A_1, Sq_1, TS_1과 해당 공격에 대한 라우터 B의 자체 보안 시스템의 대응 메시지를 주변 라우터에게 브로드 캐스팅 한다.

⑦ 초기 접속 라우터 A는 수신한 M, A_1, Sq_1, TS_1와 라우터 B의 공격 대응 메시지에서 2-MAC 인증 패킷에 대한 랜덤한 고유번호를 확인 후 자동화된 침입자 추적을 위한 자동화 프로그램을 활성화한다. 또한 공격자로부터의 MAC 주소에 해당되는 모든 IP에 대한 패킷을 차단한다.

이상의 모든 설정 후 공격자의 초기 접속시 전송되는 공격자의 2-MAC 인증 패킷에서 공격자 개인 정보의 메시지 인증 코드를 법기관에 이를 전송함으로써 추적을 완료한다.

4.4 제안 방식 검증과정

제안방식에서 계산된 추적인자 A는 다음과 같은 검증 과정을 거쳐 그 정당성을 확인할 수 있다.

$$\begin{aligned} A &= H(Z^d \bmod n) \\ &= H(S^r \times V^{r_2} \bmod n) \\ &= H((M^d)^r \times (g^d)^{r_2} \bmod n) \\ &= H[((M^r) \times (g^{r_2}))^d \bmod n] \\ &= H(Z^d \bmod n) \end{aligned}$$

5. 제안방식 분석

본 논문에서는 분산 환경에서 효율적인 공격자 추적 기법을 제안하였으며, 다음과 같이 기존 시스템과는 차별화된 특징을 가지고 있다.

① 실시간 추적 서비스

제안된 방식은 공격이 진행중이거나 완료된 상태에서도 초기 접속된 2-MAC인증 패킷을 이용한 추적 서비스가 가능하다. 이는 인증 패킷의 고유번호인 Sq의 값과 2-MAC인증 패킷에 포함된 타임 스탬프에 의해 공격의 진행 경로와 시간대별 공격 가능한 서비스를 제공한다.

$(Sq_0, Sq_1, Sq_2, \ldots, Sq_n)$ 공격 경로

$(TS, TS_1, TS_2, \ldots, TS_n)$ 대 접속 경로

② 내부 공격자에 대한 안전성

제안 방식의 경우 신뢰된 기관에 등록되어 있는 각 개체의 고유 비밀 정보의 해쉬된 개인 정보 값을 기반으로 하여 생성된 S, A의 검증을 통하여 내부 공격자에 의한 안전성을 유지할 수 있다.

③ 우회 공격의 안전성

제안된 방식은 초기 접속 라우터에서만 공격자를 차단하지 않고 우회 라우터들에 대한 브로드캐스팅 메시지 M, A, Sq를 이용한 자체 대응으로 주변 라우터들에 대한 공격자 차단을 수행한다.

④ 범용적인 추적기법 제공

제안 방식은 특정 라우터나 네트워크 장비를 통한 추적 서비스가 아닌 새로운 형태 2-MAC 인증 패킷을 초기 전송시 사용함으로써 사용자의 효율적인 추적을 제공할 수 있다.

6. 결론

본 논문에서는 기존의 네트워크 공격자 추적 기법에 대한 보안적, 효율성에 대해 분석하고 이를 보완할 수 있는 공격자 추적 기법을 제안하였다. 제안된 방식은 특정 하드웨어 장비를 필요로 하지 않으면서, 공격자에 대한 실시간적 추적 기법을 제공하였다. 그러나 지수승 연산에 따른 계산량과 신뢰기관에 개인 정보를 등록 시키고 그에 해당되는 해쉬 값을 공격자 추적 기법에 활용한다는 점에서 취약할 수 있는 요소가 된다.

따라서 본 논문에서 제안되었던 방식을 기반으로 하여 계산량과 개인 비밀 정보의 활용부분에 대한 연구를 지속적으로 수행할 예정에 있다.

7. 참고 문헌

[1] T. Sander and C. F. Tshudin, "Towards Mobile Cryptography", International Computer Science Institute TR-97-049, 1997

[2] http://www.kisa.or.kr

[3] D. S. Alexander et al., "A Secure Active Network Environment Architecture: Realization in SwitchWare", IEEE Network Magazine, 1998

[4] Dan Sterne, "Active Network Intrusion Detection and Response", Boeing and NAI Lab., DARPA DARPA FTM PI Meeting, Jul. 20. 2000

[5] D. S. Alexander et. al., "Active Network Encapsulation Protocol(ANEP)" http://www.cis.upenn.edu/~switchware/ANEP/docs/ANET.txt 1997

[6]. 이임영 "전자상거래와 보안 입문", 생능출판사 , 2001.7

[7]. Alfred J. Menezes, Paul C.van Oorschot, Scott A. Vanstone "HANDBOOK of APPLIED CRYPTOGRAPHY", CRC, 1996.11