IGMP에 대한 DoS 공격 취약점 분석 및 최소화 기법

여 동 규° 오 득 환 김 병 만 김 경 호
금 오 공 과 대 학 교 대 학 원 컴 퓨 터 공 학 과
{sylot, dhoh, bmkim, ghkim}@cespc1.kumoh.ac.kr

The Analysis of DoS Attack Vulnerability to IGMP and Minimizing Scheme

Dong-Gyu Yeo° Duk-Whan Oh Byeong-Man Kim Gyung-Ho Kim
Dept. of Computer Engineering, Graduate School, Kumoh Natl. University of Tech.

요 약

멀티캐스트 전송 필요성이 커지면서 보안에 대한 요구도 높아지게 되었다. 멀티캐스팅 라우터와 호스트간 그룹에 대한 정보를 관리하기 위해 사용되는 IGMP는 자체의 취약점이 있어서 DoS 공격이 가능하다. 본 논문에서는 이러한 IGMP 취약점과 예상되는 DoS 공격 유형을 살펴보고, 취약점 최소화를 위한 방법으로 트래픽 비율 제한 및 새로운 상태와 타이머 사용의 간단하면서도 효과적인 기법을 제안한다. 이를 위하여 라우터에 대한 하나의 상태와 네 가지의 타이머를 새로이 정의하고 동작 특성을 설명한다.

1. 서론

인터넷의 성장과 상업화는 사용자에게 매우 다양한 환경을 제공하였으며 이에 따라 멀티캐스트 전송 기술은 네트워크 대역폭과 서버스 제공자의 자원을 효과적으로 절약할 수 있는 기술로 이용되기 시작했다. 이와 더불어 보안에 대한 관심 및 요구 또한 높아지게 되었는데, 멀티캐스트 전송에 있어서의 보안은 유니캐스트에 비해 보다 복잡하기 때문에 멀티캐스팅 보안에 관한 연구가 활발히 진행되고 있다.

멀티캐스트 전송에서의 보안 구조에 결정적인 영향을 미칠 수 있는 요소는 여섯 개이며[1], 이 중에서도 특히 송신자는 수신자가 누구인지 모른다는 것과 라우터에서의 별도의 추가적인 패킷 해석 및 중계 처리가 필요하다는 점을 이용하여 해당 네트워크에 트래픽 폭주를 유발시키는 DoS(Denial of Service) 공격이 가능하다. 이러한 취약점은 라우터간 멀티캐스팅 프로토콜에서보다 종단 멀티캐스팅 라우터와 호스트간 그룹 멤버쉽 정보를 교환하는 IGMP(Internet Group Management Protocol)에서 보다 심각하게 나타날 수 있다.

현재까지 멀티캐스팅 통신에서 보안에 관련되어 진행되고 있는 연구는 주로 각 그룹에 대하여 고유한 키를 만들고 이를 이용한 송·수신자 인증 및 암호화 통신을 하는 기법들이다[2][4][5]. 하지만 이러한 그룹 키 관리 기법은 키를 주기적으로 갱신하여야 하고 또한 암호화 및 복호화 과정을 거쳐야 하므로 전송 지연 시간 등의 문제 때문에 DoS 방지 기법으로 실제 적용하기에는 무리가 있다.

DoS 공격에 방어하기 위해서는 라우터나 방화벽을 이용한 패킷 필터링 기법 등이 이용되고 있으나 뚜렷한 해결책이 없는 것이 현재의 실정이므로, 프로토콜 자체의 문제점을 제거하는 것이 가장 효과적이다.

본 논문에서는 IGMP가 가지고 있는 DoS 공격에 대한 보안상 취약점을 분석하고 이를 해결하기 위해 간단한 기법을 사용하여 효과적으로 멀티캐스트 트래픽 폭주를 막으며 IGMP의 근본적인 취약점을 최소화할 수 있는 기법을 제안한다.

2장에서는 관련 연구를 개괄적으로 설명하며 3장에서는 IGMP의 취약점을 분석하고 예상되는 DoS 공격 유형을 살펴본다. 4장에서는 취약점을 최소화하기 위해 제안한 기법을 설명하며, 5장에서 결론을 맺고 향후 연구 방향에 대해 논의한다.

2. 관련 연구

2.1 IGMP(Internet Group Management Protocol)

IGMP는 멀티캐스팅 데이터를 수신하고자 하는 호스트가 특정 그룹에 대한 자신의 멤버쉽 정보를 보유하고 있는 이웃한 멀티캐스팅 라우터에게 보고하는데 사용되는 프로토콜이다[3].

라우터는 주기적으로 서브넷에 일반 질의(General Query) 메시지를 보내고, 호스트는 이에 대한 응답으로 자신의 멤버쉽을 보고(Report) 한다. 또한 호스트가 그룹에서 탈퇴(Leave)하고자 할 때는 탈퇴 메시지를 보내며, 라우터는 더 이상 멤버가 없는지 확인하기 위하여 그룹-지정 질의(Group-Specific Query) 메시지를 여러 번 보낸다. 이 때 호스트로부터 보고 메시지가 오지 않아 더 이상의 멤버가 없다는 것이 확인되면 라우터는 해당 그룹에 대한 패킷 중계를 중단하게 된다. 이 과정을 그림으로 도시하면 **그림 1**과 같다.

라우터는 **그림 1**과 같은 방법으로 호스트와 통신하여 각 그룹에 대한 멤버쉽을 결정하며, 자신이 중계해 주어야 할 그룹들의 리스트를 관리한다. 또한 효율적으로 멤버쉽 정보를 전달하기 위하여 라우터는 여섯 개의 타이머와 세 개의 카운터를 호스트는 두 개의 타이머를 이용한다[3].

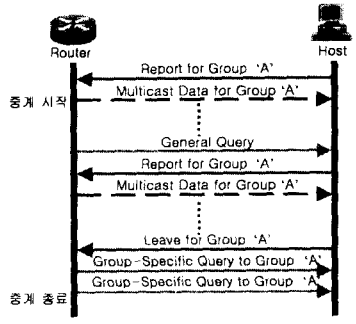

그림 1. 라우터와 호스트간 멤버쉽 판단

2.2 DoS(Denial of Service) 공격

서비스 거부 공격이란 한 사용자 또는 프로세스가 멀티태스킹 시스템 하에서 리소스를 독점하여 사용하거나 파괴함으로써 다른 사용자 또는 프로세스들이 올바른 서비스를 제공받지 못하게 하는 공격법으로서, 정상적인 수행에 문제를 야기하여 올바른 서비스가 불가능하게 하기 때문에 ISP에게는 치명적인 공격법이 될 수 있다. 이러한 DoS 공격은 감지하기도 어렵고 문제점을 해결하기도 어려우며 아주 다양한 변형 방법들이 가능하다.

이에 대응하기 위한 방안으로는 시스템의 리소스를 한 개인이나 프로세스가 독점하지 못하도록 설정한다거나, 취약점을 제거한 패치 프로그램 또는 최신 프로그램을 이용할 수 있으며, 라우터나 방화벽을 이용한 패킷 필터링 방법이 사용되기도 한다.

3. 예상되는 DoS 공격 유형

3.1 모든 그룹에 대한 보고 공격

공격자가 모든 그룹에 대하여 멤버쉽 보고 메시지를 보내는 방식의 공격이 가능하다. 이 경우 라우터는 각 그룹에 대하여 현재 상태를 저장하고, 각 그룹에 대하여 여러 개의 타이머를 관리하기 시작한다. 또한 모든 그룹의 데이터 스트림을 서브넷으로 중계해 주게된다. 그런데 최악의 경우 계산상 멀티캐스팅의 가능한 전체 그룹의 수인 2^{28} 개의 그룹이 액티브 상태이고 각 그룹에 대해 송신자가 여러 곳이라면 라우터에 부하가 많이 올라갈 뿐만 아니라 해당 네트워크의 트래픽이 급속히 증가하게 되어 네트워크가 마비된다.

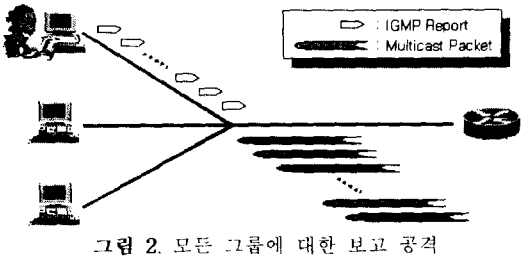

그림 2. 모든 그룹에 대한 보고 공격

3.2 모든 그룹에 대한 지속적인 가입 및 탈퇴 공격

공격자가 모든 그룹에 대하여 지속적으로 가입 및 탈퇴를 반복하는 유형으로 공격한다. 이 경우 역시 라우터는 각 그룹에 대하여 상태 및 타이머를 관리하며 데이터 스트림을 중계해 주기 시작한다. 특히 탈퇴 메시지에 대해서는 더 이상 멤버가 존재하지 않는지 확인하기 위하여 그룹-지정 질의 메시지를 보내게 되며, 또한 이에 대해 각 호스트들은 타이머를 작동시켜 자신들의 멤버쉽을 보고하게 되는 추가의 트래픽이 발생한다. 모든 그룹에 대한 보고 공격의 경우보다 더 강한 공격 유형으로서 역시 트래픽을 심각하게 증가시키며, 더불어 라우터와 호스트 모두에게 별도의 처리를 요구한다.

3.3 위조된 질의 공격

공격자가 현재의 질의자보다 낮은 IP 주소를 가지고 질의 메시지를 보내면 질의자 선출 규칙에 의거하여 공격자 호스트가 새로운 질의자가 되고 기존의 질의자 역할을 하던 라우터는 비질의자(Non-Querier) 상태로 들어가게 된다[3][6]. 공격자는 다시 자신을 비질의자의 상위 멀티캐스팅 라우터와 터널을 연결해서 자신이 속한 서브넷으로의 멀티캐스팅 패킷 중계 역할을 맡게 된다. 질의자는 터널을 통하여 수신된 추상 멀티캐스팅 패킷(Encapsulated Multicasting Packet)을 실제 멀티캐스팅 패킷으로 가공하여 서브넷으로 중계해 주어야 하는데, 이때 질의자가 된 공격자가 주기적으로 질의 메시지를 보내기는 하지만 데이터 스트림을 서브넷으로 중계하지 않는다면 그룹의 멤버들은 전혀 데이터를 수신하지 못하는 비정상적인 서비스 상태가 된다.

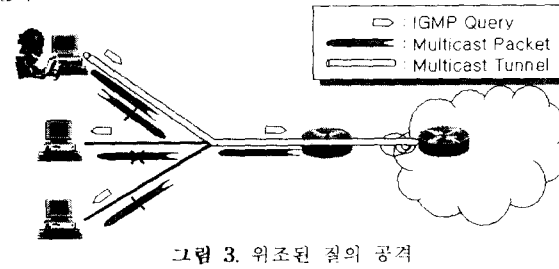

그림 3. 위조된 질의 공격

4. 제안된 IGMP 취약점 최소화 기법

본 장에서는 3장에서 분석한 IGMP의 보안상 취약점을 최소화하기 위하여 제안한 기법에 대해 설명한다. 꺾쇠 괄호([ ])는 본 논문에서 새롭게 정의한 타이머(카운터)를 의미하며 산형 괄호(< >)는 기존 IGMP 명세의 것을 의미한다.

본 논문에서는 다음과 같은 조건을 가정한다.

(1) 다수 그룹이 액티브하며 트래픽도 많은 상태이다.
(2) 주 공격 위치는 서브넷 내부이다.
(3) 내부공격자는 외부 라우터와 터널링이 가능하다.
(4) 라우터 및 호스트의 행동은 명세(RFC2236[3])를 따른다.

4.1 모든 그룹에 대한 보고 공격 방지

이러한 유형의 공격은 멀티캐스팅의 전체 트래픽 양을 제한함으로써 방지할 수 있다. 라우터는 패킷 전달 지연 시간을 측정하여 허용치 이상을 넘어가면 더 이상의 새로운 그룹에 대한 가입을 무시하도록 한다. 이를 위하여 라우터는 **[지연 측정 (Latency Measure Interval)]** 타이머가 소진될 때마다 외부로부터 라우터에 도착하는 임의의 멀티캐스팅 패킷이 라우터를 빠져나갈 때까지의 전달 지연 시간을 측정하여 **[허용 지연 (Allowed Latency)]** 을 초과하게되면 더 이상의 새로운 그룹에 대한 보고를 무시함으로써 트래픽의 증가를 막는다. 또한 라우터가 최대의 성능으로 동작하고 있더라도 기존 그룹에 대하여 송신자가 증가하거나 유니캐스팅 트래픽이 증가하는 등의 원인으로 패킷 전달 지연 시간이 허용치 이상을 넘어갈 경우 QoS 메커니즘에 의해 희생시킬 그룹 또는 송신자를 선정하여 트래픽을 조절해야 한다. [지연 측정] 및 [허용 지연] 은 네트워크의 특성 및 장비의 능력에 따라 관리자가 쉽게 변경하거나 동적으로 변화될 수 있어야 한다. 질의자 상태 변화를 위해 다

음 이벤트와 액션, 변수가 추가된다.

(1) "allowed latency variable" 변수
(2) "latency measure timer expired" 이벤트
(3) "over latency" 이벤트
(4) "start latency measure timer" 액션
(5) "forcible leave" 액션

4.2 모든 그룹에 대한 지속적인 가입 및 탈퇴 공격 방지

라우터가 탈퇴 메시지를 수신하면 <잔여 멤버 질의(Last Member Query Interval; 디폴트 1초)> 타이머가 소진될 때마다 <잔여 멤버 질의 횟수(Last Member Query Count; 디폴트 2)> 만큼 그룹-지정 질의 메시지를 보내고, 호스트는 해당되는 그룹에 대한 <보고 지연 타이머(Report Delay Timer; 1초 이내)> 를 작동시켜 멤버쉽을 보고한다[3].

이러한 추가적인 동작과 트래픽을 줄이기 위해 각 그룹에 대해 <그룹 멤버쉽 유효(Group Membership Interval; 디폴트 350초)> 타이머 외에 **[그룹 멤버쉽 생존(Group Membership Life Interval)]** 타이머를 두어 이 구간 내에서는 탈퇴 메시지를 무시하도록 한다. 이 타이머의 값은 보고 메시지를 수신할 때마다 초기값으로 갱신된다. <그룹 멤버쉽 유효> 또한 보고 메시지를 수신할 때마다 초기값으로 갱신되기 때문에 [그룹 멤버쉽 생존] 의 초기값은 <그룹 멤버쉽 유효> 타이머 값의 일정 비율을 이용할 수도 있다. 이 기법은 모든 그룹에 대한 지속적인 보고 공격 방지 기법과 병행해야 한다. 질의자 상태 변화를 위해 다음 액션이 추가된다.

(1) "start membership life timer" 액션
(2) "reset group membership life timer" 액션

4.3 위조된 질의 공격 방지

비질의자가 된 라우터는 중계는 하고 있지 않지만 상위 멀티캐스팅 라우터와 터널링이 되어 있기 때문에 멀티캐스팅 패킷을 수신할 수 있으며, 또한 서브넷 호스트의 IGMP 보고 패킷도 수신할 수 있어서 언제라도 질의자가 될 수 있도록 멤버쉽 리스트를 관리하고 있다[3][6].

이와 같은 성질을 이용하여 비질의자가 된 라우터는 현재 각 액티브 그룹에 대한 **[중계 감시(Route Monitor Interval)]** 타이머를 작동한 후, 네트워크를 감시하여 각 액티브 그룹에 대한 [중계 감시] 타이머가 소진될 때까지 액티브 상태의 그룹에 대한 패킷이 질의자에 의해 중계가 되지 않는다면 자신을 본 논문에서 새로이 정의한 **강제 중계자(Forcible Router)** 임무 상태로 변환한다. 이 때 해당 그룹의 [중계 감시] 타이머 작동을 중지한 후 해당 그룹에 대한 중계를 시작한다. 강제 중계자 상태에서는 자신보다 낮은 IP 주소에서의 질의 메시지로 인하여 비질의자 상태로 변환하지는 않는다. 이 [중계 감시] 타이머는 패킷이 중계되고 있는 것을 확인할 때마다 갱신된다.

만일 강제 중계자 상태에서 중계중인 그룹의 패킷을 질의자가 중계하는 것을 발견하면, 즉시 해당 그룹에 대한 중계를 중단하고 [중계 감시] 타이머를 작동한다.

만일 강제 중계자 상태에서 모든 액티브 그룹에 대해 [중계 감시] 타이머가 작동하게 되면 비질의자 상태로 변환한다.

강제 중계자 상태에서 질의자 상태로의 변환은 비질의자 상태에서 질의자 상태로의 변환과정과 동일하게 <다른 질의자 존재(Other Querier Present Interval)> 타이머에 따른다.

라우터 상태 변화를 위해 다음 이벤트 및 액션이 추가되고, 라우터 상태도는 **그림 4**와 같이 확장된다.

(1) "route monitor timer expired" 이벤트
(2) "all monitor timer started" 이벤트
(3) "notify real routing +" 액션

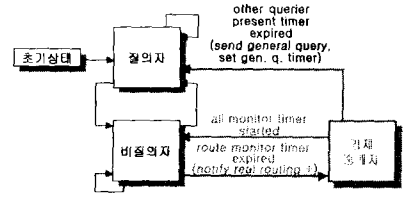

그림 4. 확장된 라우터 상태도

강제 중계자를 위해 다음 이벤트 및 액션이 추가된다. 비질의자의 상태도를 확장하여 이루어지는 강제 중계자의 상태도는 **그림 5**와 같다.

(1) "routed multicast packet received from other querier" 이벤트
(2) "start route monitor timer" 액션
(3) "notify real routing -" 액션

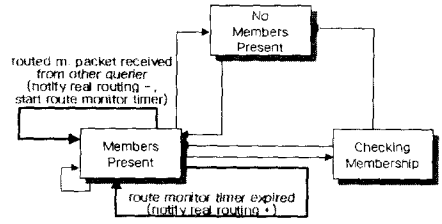

그림 5. 강제 중계자 상태도

5. 결론 및 향후 연구 과제

상용 멀티캐스팅 서비스 시스템에 대한 DoS 공격은 어렵지 않은 공격이면서도 매우 치명적인 해킹 공격법이다. 본 논문에서 제안한 새로운 상태와 타이머들을 이용하여 IGMP 취약점을 최소화하면 예상되는 DoS 공격을 최소화할 수 있으며 IGMP의 라우터 구현만 확장하면 되므로 매우 효과적이다.

기술한 공격 유형 외에도 다양한 공격 방법이 가능하다. 위조된 질의자가 내용을 변조하여 중계하거나, 복제 또는 변조한 내용으로 다수의 새로운 그룹을 만들어 트래픽 폭주를 유발할 수도 있다. 이러한 문제점을 해결하기 위해 그룹 키 관리를 통한 송신자 인증 메커니즘이 현재 계속 연구되고 있는데, 앞으로의 연구 방향은 제안된 기법을 그룹 키 관리 기법 및 QoS 메커니즘과 효율적으로 연결하여야 하며 또한 라우터가 아닌 방화벽 시스템에 적용시키는 방법도 연구되어야 한다. 그리고 새로운 타이머와 카운터의 적절한 디폴트 값을 산정해야 하며, 고속처리를 요하는 라우터에서 빠르게 접근하고 수정할 수 있게 하여야 한다.

6. 참고문헌

[1] R. Canetti, B. Pinkas, "A taxonomy of multicast security issues", INTERNET-DRAFT, April 1999.
[2] IRTF Secure Multicast Group(SMuG), http://www.ipmulticast.com/community/smug/
[3] W. Fenner, "Internet Group Management Protocol, Version 2", RFC2236, November 1997.
[4] T. Hardjono, R. Canetti, M. Baugher, P. Dinsmore, "Secure IP Multicast: Problem Areas, Framework and Building Blocks", INTERNET-DRAFT, October 1999
[5] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC2401, November 1998
[6] Thomas A. Maufer, "Deploying IP Multicast in the Enterprise", Prentice Hall, 1998