제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

# 결함허용 네트워크에 대한 연구

김기한*, 김홍철*, 정주영*
*국가보안기술연구소
e-mail : ghkim1@etri.re.kr

# A Study on Fault Tolerant Network

GiHan Kim *, HongChul Kim*, JuYoung Jung*
*National Security Research Institute

요 약

기존의 보안 관점에서의 정보보호는 암호화, 인증과 접근제어를 이용하여 권한없는 접근을 방지하는 부분과 침입탐지와 같은 수동적인 관점에서 많이 연구되었다. 그러나 프로그램의 계속적인 취약성이 발견됨에 따라 보다 적극적인 방어 개념인 정보 생존성에 대한 연구도 활발히 이루어지고 있다. 본 논문에서는 정보 생존성에서 네트워크 관점에서 고장 또한 침입에 의한 결함에도 지속적인 네트워크 서비스를 제공할 수 있는 결함허용 네트워크에 대한 아키텍처를 제시한다.

## 1. 서론

분산환경에서 결함허용 기법은 많이 연구되었고 현재도 지속적으로 진행 중에 있다. 컴퓨터 시스템에서 결함과 관계된 신뢰성을 향상시키는 주된 두가지 방법은 결함방지와 결함허용이다. 그러나 결함방지 기법은 사전에 모든 결함을 방지해야 하므로 현실적으로 불가능한 점이 존재하고 보안관점에서 취약성을 이용한 공격에 대해서는 최선의 선택이 아니다. 그러므로 소프트웨어의 취약성을 이용한 공격과 서비스 거부 공격과 같은 경우에도 지속적인 네트워크 서비스를 제공해줄 수 있는 결함허용 네트워크에 대한 연구는 필수적이다.

기존의 결함허용 연구는 복제의 증가를 수행하여 가용성을 향상하는 접근법이 많이 존재한다[1]. 네트워크 환경에서 결함허용을 수행하기 위해서는 결함허용을 위한 복제 뿐만 아니라 보안에 필요한 기밀성 간에 상호작용이 필요하다. 왜냐하면 결함 회복 매커니즘도 공격자에 의해 악용될 수 있는 취약성이 존재하기 때문이다. 또한 복제의 증가는 취약성이 증가되어 보안관점에서의 기밀성에 대한 위협이 증가하는 문제가 존재한다.

결함허용 생존 네트워크 기술은 위에서 언급한 고장과 침입에 대해 둘 다 고려를 하여 단순 복제를 이용한 결함허용 기법 이외에 기밀성에 대한 상호작용도 고려되어야 한다.

결함허용 네트워크는 공격이 성공하더라도 지속적인 네트워크 동작을 제공해줄 수 있는 기술을 개발한다. 또한 네트워크 레벨에서 결함허용 능력을 가지게 하여 무결성과 가용성을 보장하는 기술을 포함한다.

본 논문에서는 이러한 결함허용 네트워크에 대한 분석을 통해 결함허용 네트워크에서 필요한 기능을 추출하고 결함허용 네트워크에서 필요한 기술에 대한 아키텍처을 제시하는데 목적을 둔다.

본 논문의 구성은 2 장에서 DARPA 에서 연구중인 결함허용 네트워크 프로젝트에 대해 알아보고 3 장에서 결함허용 네트워크 아키텍처를 제시하고 4 결론을 맺는 구성이다.

## 2. DARPA IA&S 의 결함허용 네트워크 프로그램

DARPA 의 IA&S(Information Assurance and Survivability) 프로젝트는 정보전에 대응하기 위한 정보 보증 및 생존 기술 개발을 주도하고 있다. 그 주요 내용은 여덟 가지 영역에 걸쳐 전략적 침입평가(Strategic Intrusion Assessment), 침입감내 시스템(Intrusion Tolerant Systems), 결함허용 네트워크(Fault Tolerant Networks), 동적협동(Dynamic Coalitions), 정보 보증(Information Assurance), 정보 보증 과학 및 공학 도구(Information Assurance Science and Engineering Tools), 자율적 정보 보증(Autonomic Information Assurance), 그리고 사이버 지휘 통제(Cyber Command and Control) 기

술을 개발하는 것이다.

이 중 결함허용 네트워크와 침입감내 시스템은 정보 생존성에서 침입을 감내하는 메커니즘을 제공해주는 영역이다. 침입감내 시스템은 호스트 레벨에서 제공되는 서비스에 대한 지속적인 제공을 강조하고 있으나 결함허용 네트워크는 네트워크 레벨에서 네트워크 서비스를 지속적으로 제공하는 것을 목표로 하고 있다[2] . 즉 결함허용 네트워크 프로그램은 공격이 성공하더라도 지속적으로 올바른 네트워크 동작을 수행하기위한 기술을 개발한다. 또한 침입감내 시스템 프로그램에서 이미 개발된 기술을 네트워크에 적용하는 기술도 수행한다. 호스트에 공격이 진행되는 동안 피해를 최소화하고 네트워크의 최소한 기능을 유지하게 해야 한다. 그리고 결함허용 프로그램은 네트워크 레벨에서의 공격에 대해서도 결함허용을 수행해야 하고 대표적인 예로 서비스 거부 공격 에 대해서도 잠재적인 취약성을 줄이는 기술과 Active network 를 사용하는 공격 대응 기술을 포함하여 연구가 진행 중에 있다.

이와 같이 DARPA 의 IA&S 프로젝트의 결함허용 네트워크 프로그램은 결함허용 생존 네트워크, 서비스 거부 공격의 대응, Active network 에서의 결함허용의 세가지 부분으로 분류하고 있다.

DARPA IA&S 프로그램의 구체적인 목표는 다음과 같다.

- 네트워크 서비스에 대한 결함허용과 보안 생존성 강화
- 공격자가 사용하는 리소스를 제한하여 서비스 거부 공격의 대응
- 현재 네트워크에 대한 이해 향상의 관점에서의 공격자에 대한 추적

## 3. 결함허용 네트워크 아키텍처

이 장에서는 결함허용 네트워크를 위한 전체적인 구성을 제시하고 있다.

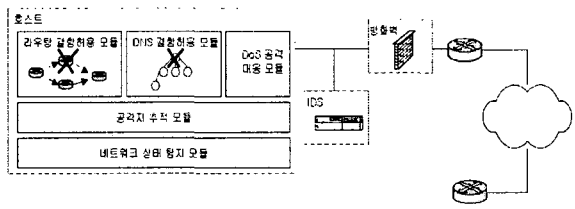
네트워크 서비스에 대한 공격은 세가지로 구분할 수 있다. 첫번째는 악의적인 라우팅 정보를 제공하는 공격법과 두번째는 악의적인 DNS 서버를 이용하여 사용자의 요구를 다른 호스트로 이동할 수 있는 공격법과 세번째는 서비스 거부 공격이다.

현재 라우팅 프로토콜은 내부 네트워크에서 라우팅 정보를 교환하는 데 사용하는 RIP, OSPF 등이 존재하고 외부 네트워크에서 라우팅 정보를 교환하는 BGP 등이 존재한다. 그러나 이러한 라우팅 프로토콜은 인증이 없는 버전도 존재하고 인증과정이 존재하더라도 비밀번호가 평문으로 전송되는 문제점도 존재한다. 그러므로 이러한 라우팅 프로토콜을 보완하여 네트워크의 공격이 수행되더라도 결함허용성을 가질 수 있는 새로운 메커니즘의 개발이 필요하다.

두번째는 악의적인 DNS 을 이용하는 공격으로서 악의적인 DNS 서버를 운영하여 호스트 이름에 대한 IP 매핑을 잘못된 정보를 제공할 수 있고 다른 접근법으로 DNS 의 root 서버를 공격을 하여 마비가 된 경우 호스트 이름으로 통신을 수행하는 네크워크 서비스의 많은 부분이 서비스를 제공하지 못하는 문제점도 발생할 수 있다. 현재의 인터넷 뿐만 아니라 폐쇄망에서 DNS 서버를 운영을 하고 있는 경우에 루트 DNS 가 내부자의 공격이든 고장에 의한 결함에 의한 마비를 고려해야 하고 이러한 문제을 극복하기 위해 DNS 에서도 결함허용성을 가지게 하는 메커니즘의 개발도 필요하다.

세번째는 서비스 거부 공격에 대한 대응이다. 서비스 거부 공격에 대한 추적에 어려움 점은 IP spoofing 에 따른 소스 IP 추적이 어렵다는 점이다. 네트워크 상태를 인식한 상태에서 이러한 IP spoofing 을 파악하여 공격지를 파악을 하면 서비스 거부 공격을 완화할 수 있는 메커니즘을 적용할 수 있다. 이 뿐만 아니라 QoS 를 지원하는 네트워크 프로토콜에 대한 서비스 거부 공격과 무선 환경의 ad hoc 네트워크에 대한 서비스 거부 공격의 대응에 대한 연구도 필요하다.

그림 1 에 전체적인 결함허용 네트워크의 구성도가 표현되어 있다.




(그림 1) 결함허용 네트워크 아키텍처

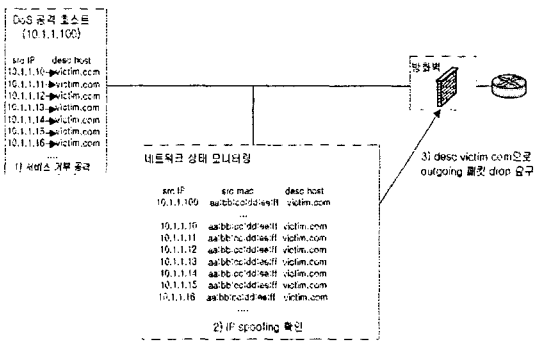
### 3.1 네트워크 상태 탐지 모듈

현재의 IDS 의 대부분 설치 위치는 ISP 와 조직 내부 네트워크의 경계 라우터, 방화벽 다음에 위치하게 되어 스위치 허브를 사용하는 경우 포트 미러링을 이용하여 조직의 네트워크 내부로 들어오는 패킷에 대해 검사와 감사 기록을 남기는 기능을 수행한다. 그러나 IDS 는 IP 주소 기반의 패킷을 주로 탐지하기 때문에 IP spoofing 을 이용한 공격에는 공격지 추적에 어려움이 많이 존재한다. 현재 일부 방화벽에서는 이러한 IP spoofing 을 방지하는 기능이 포함되어 있고 방화벽 로그로 남길 수 있다. 분산 서비스 거부 공격을 예를 들면 이러한 IP spoofing 은 공격을 수행하는 서비스 거부 에이전트에서 많이 사용하는 기법이고 이러한 패킷은 서비스 거부 공격이 수행되는 네트워크에 실시간으로 방지됨이 분산 서비스 거부 공격의 대응에 적합하다.

그리고 방화벽에서 수행하는 IP spoofing 방지 기능도 내부 네트워크의 IP 를 가지고 spoofing 을 수행하는 경우 spoofing 을 막기 어려울 수 있다. 그러므로 내부 네트워크에서 mac address 에 대한 빈번한 IP 변경을 조사하여 내부 네트워크 내부에서 IP spoofing 을 체크하여 IP spoofing 을 방지하는 기능도 필수적이다. 이 같은 모니터링 기능을 수행하는 arpwatch[3]의 경우 mac address 와 IP address 에 대한 변경 사항을 email

로 전송해주는 프로그램이다. 네트워크 상태 탐지 모듈에서는 이러한 arpwatch 프로그램과 유사하게 지속적으로 mac address 와 IP address 에 대한 모니터링을 통해 너무 빈번한 변화가 오는 호스트는 서비스 거부 공격을 수행하는 호스트로 볼 수 있고 그 호스트의 out-bound 통신을 막아야 한다.

그림 2 에 내부 네트워크에서의 IP spoofing 방지에 대한 구조가 표현되어 있다.




(그림 2) 내부 네트워크에서의 IP spoofing 방지

이러한 서비스 거부 공격 뿐만 아니라 DNS 에 대한 질의 기록과 응답 기록, 라우팅 프로토콜에 대한 기록도 남겨 라우팅 결함허용 모듈과 DNS 결함허용 모듈에 입력 자료로 사용 가능하게 기록이 남겨져야 한다.

### 3.2 공격자 추적 모듈

공격자 추적 모듈은 실시간 공격자 추적을 제공하기 위해 IDS, 방화벽의 감사로그 뿐만 아니라 네트워크 상태 탐지 모듈의 정보를 이용하여 공격지에 대한 질의를 보내면 공격지를 확인하는 기능을 수행한다.

이러한 공격자 추적 모듈이 필요한 이유는 공격을 수행하는 IP 가 중간 경유지인 경우가 많이 존재하기 때문에 실제 공격자가 위치한 공격지를 알 수 없는 경우가 많이 존재하기 때문이다.

공격자 추적은 실시간으로 이루어져야 하고 IDS, 방화벽의 감사로그와 네트워크 상태 탐지 모듈의 감사로그를 통합하여 연결이 이루어진 공격자 추적 모듈에 질의와 검색하여 실제 공격 시작점을 찾아내는 메커니즘이 필요하다.

또한 서비스 거부 공격의 적극적인 대응으로 서비스 거부 공격의 완화를 위해 역 서비스 거부 공격을 수행하고자 하는 경우에도 IP spoofing 으로 위장된 서비스 거부지를 정확하게 찾아내는 기능은 필수적이다.

### 3.3 라우팅 결함허용 모듈

라우팅 프로토콜에 대한 공격을 수행하면 라우팅 이웃관계를 끊어 원할한 통신이 불가능하게 만들거나 반복적인 라우팅 정보 메시지를 전송하여 특정 경로에 부하를 주는 공격, 비정상적인 라우팅 경로를 삽입하여 특정 네트워크에 도달하지 못하게 하는 공격 등이 존재할 수 있다.

첫번째로 단순한 보안 정책은 내부 네트워크에서 라우팅 프로토콜을 사용할 수 있는 호스트를 정해두고 이 호스트가 아닌 내부 호스트에서 라우팅 프로토콜을 사용하는 경우 이를 공격으로 인식하는 방법을 고려할 수 있다.

그러나 이러한 단순 보안 정책으로는 감사기록만 남길 수 있고 라우팅에 대한 결함허용성은 가질 수 없다. 그러므로 기존의 라우팅 프로토콜의 확장을 통해 이러한 결함허용성을 가지도록 하는 방법과 인터넷 라우팅 방법을 기반으로 새로운 라우팅과 패스를 제공해주는 새로운 메커니즘을 제시하는 방법으로 구분될 수 있다.

### 3.4 DNS 결함허용 모듈

결함허용 네트워크를 제공하기 위해서는 라우팅에 관계한 결함허용성 뿐만 아니라 호스트 이름을 이용하여 네트워크 서비스를 제공하는 경우 DNS 에 대한 결함 허용성은 매우 중요하다. root DNS 에 대한 공격이 성공한 경우 호스트 이름을 이용하는 네트워크 서비스는 제대로 동작할 수 없다.

DNS 는 고장과 같은 환경에 대비하여 master DNS 와 여러대의 secondary DNS 로 분산 운영될 수 있다. 그러나 현재의 DNS 는 공격의 대상이 될 네임서버가 해커의 네임서버에 질의를 하도록 하여 악의적인 도메인 네임 정보를 제공하는 공격이 존재한다. 이러한 문제는 DNS 의 설정을 변경을 통해 해결할 수 있으나, 보다 향상된 보안 기능을 제공하기 위해 네임 서버간에 통신을 안전하게 하는 용도로 DNSSEC[4]이 개발되어 있다. 이 DNSSEC 은 PKI 을 이용하여 영역관리자가 자신의 영역 데이터에 서명을 하여 전송을 하기 때문에 안전한 영역 정보의 전송을 제공할 수 있다. 그러나 이러한 DNSSEC 은 고장과 결함에 대한 부분은 고려되지 않고 있는 문제점이 있다.

그러므로 트리 모양의 도메인 네임에서 root DNS 에 대한 고장에 대해 하부 coordinater 들이 새로운 root DNS 용 결정하여 DNS 의 결함허용성을 보장해줄 수 있는 기능도 필요하다. 만약 폐쇄망인 경우라도 방대한 네트워크를 사용하고 DNS 을 분산 운영하는 경우에는 이러한 DNS 에 대한 결함허용성은 필요하다.

### 3.5 서비스 거부 대응 모듈

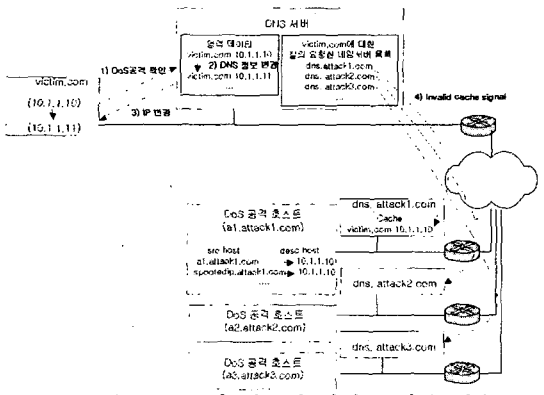
서비스 거부 대응 모듈은 네트워크 상태 탐지 모듈의 필수적인 기능인 IP spoofing 으로 해결할 수 있다. 그러나 모든 네트워크에 내부 네트워크에서 내부 IP spoofing 된 패킷을 막아야한다는 가정이 필수적이다. 현실적으로 모든 네트워크에 네트워크 상태 탐지 모듈을 설치하는 것은 불가능 할 수 있다. 그리하여 피해쪽 네트워크에서의 서비스 거부 대응 메커니즘도 필요하다.

서비스 거부 대응에 대응은 기존의 연구로서는 서비스 거부 공격의 완화를 위해 서비스 거부 공격을 수행하는 호스트의 네트워크 자원을 소비하여 공격을 완화시키는 역 서비스 거부 공격 방법이 존재한다. 이

러한 역 서비스 거부 공격은 공격지가 어디 인지 정확하게 파악해야 하는 것이 중요하다. 이러한 공격지 추적은 공격지 추적 모듈에 질의를 통하여 알아낼 수 있다.

이와 다른 접근법으로 서비스 거부 대응을 살펴보면 DNS 와 접목한 서비스 거부 대응 방법을 고려할 수 있다.

그림 3 에 DNS 와 접목된 서비스 거부 대응에 대한 구성이 표현되어 있다.




(그림 3) DNS 와 접목된 서비스 거부 대응

서비스 거부 공격은 서버를 공격하여 서버에서 제공하는 서비스를 불능상태로 만드는 공격이다. 서버는 대부분 DNS 서버에 호스트 이름을 등록하여 사용하고 있다. 서비스 거부 공격을 특정 IP 에 대해 수행할 수도 있다. 서비스를 제공하는 호스트의 IP 가 변경될 수 있으므로 장기적인 관점에서의 서비스 거부 공격은 호스트 이름을 가지고 수행할 것이다. 이와 같이 도메인 호스트 이름을 이용한 경우에서 서비스 거부 대응 방법은 DNS 의 영역 데이터를 실시간을 갱신하여 공격을 받는 IP 을 변경하는 방법으로 서비스 거부 공격을 회피할 수 있다.

그림 3 에서 victim.com 의 DNS 서버는 처음에 victim.com 이 10.1.1.10 이란 IP 을 가진다라고 저장되어 있다. 만약 a1.attack1.com 과 a2.attack2.com, a3.attack3.com 의 호스트에서 victim.com 으로 서비스 거부 공격을 수행하고자 하는 경우 자신의 네임서버에 *victim.com* 의 IP 주소를 질의하게 되고 dns.attack1.com, dns.attack2.com, dns.attack3.com 은 victim.com 의 DNS 서버에 질의를 수행하여 victim.com 의 IP 주소를 알아내고 그 값을 네임서버에 설정 값에 따라 캐쉬에 보관을 한다.

a1.attack1.com 와 a2.attack2.com 과 a3.attack3.com 은 10.1.1.10 으로 서비스 거부 공격을 수행하고 victim.com 은 자신의 네트워크 리소스를 주기적으로 확인한다면 자신이 서비스 거부 공격을 당하는지를 확인할 수 있다. 그 후 DNS 에게 자신이 서비스 공격을 받음을 알리게 된다. DNS 서버는 victim.com 의 IP 를 10.1.1.20 으로 서비스 공격이 발생하지 않는 IP 로 변경을 수행하고 victim.com 의 IP 를 변경하라는 시그널을 발생한다. 그러고 나서 자신에게 victim.com 의 IP 를 질의한 네임서버에 캐쉬값이 틀렸다는 사실을 공지해주어야 한다. 이러한 캐쉬값이 틀렸다는 사실은 현재의 DNS 서버의 기능을 확장하여 구현하여야 한다.

이런 방법으로 DNS 서버에 대한 기능 확장과 실시간 IP 변경을 수행하면 서비스 거부 공격을 수행하는 a1.attack1.com, a2.attack2.com, a3.attack3.com 은 지속적으로 10.1.1.10 에만 공격을 수행함으로 victim.com 는 지속적인 서비스를 제공해줄 수 있다.

이외에도 현재까지 공격사례가 존재하지 않지만 RSVP(Resource ReSerVation Protocol)과 IntServ(Intergrated Services), DiffServ 와 같은 QoS 를 지원하는 프로토콜에 대한 서비스 거부 공격에 대한 대응하는 기술과 무선 네트워크에서 사용되는 ad-hoc 네트워크에서의 서비스 거부 공격에 대한 대응 기능이 지원되어야 한다.

## 4. 결론

본 논문에서는 보다 적극적인 방어의 개념인 생존성 관점에서 결함허용 네트워크의 아키텍처를 제시하였다. 결함허용 네트워크에서 중요한 부분은 네트워크의 서비스의 지속적인 제공을 목표로 하고 있으므로 현재 라우팅 프로토콜의 확장 및 IP 기반의 라우팅 프로토콜 상위에 새로운 라우팅 패스를 제공하는 메커니즘의 개발이 필요하다.

Sendmail 과 같은 호스트 이름에 기반하여 서비스가 이루어지는 경우를 위해 서 DNS 에 대해서도 결함허용성을 가지도록 하는 기술도 포함된다.

그리고 서비스 거부 공격에 대한 대응부분도 결함허용 네트워크에서 중요한 부분으로 로컬 네트워크에서의 IP spoofing 을 방지하고 DNS 을 이용하여 IP 의 동적 변경을 수행하여 서비스 거부 메커니즘을 방지하는 기능을 설명하였다.

향후 연구과제로는 생존성의 완전한 모습을 위해서 호스트에 결함허용성을 향상시키는 연구인 침입감내 시스템과 네트워크의 결함허용성을 향상시키는 연구인 결함허용 네트워크의 유기적 통합에 관한 연구가 필요하다.

## 참고문헌

[1] R. Chow, *Distributed Operating System & Algorithm*, pp. 425-426, Addison Wesley, 1997.
[2] http://www.afrlsn.afrl.af.mil/IA&S_topics.html#FTN
[3] ftp://ftp.ee.lbl.gov/arpwatch.tar.gz
[4]http://www.ietf.org/html.charters/OLD/dnssec-charter.html