TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx/R1 제(개)정일: 20xx년 xx월 xx일

TTAx.xx-xx.xxxx/R1-Cor1 오류정정일: 20xx년 xx월 xx일

능동적 네트워크 방어 서비스를 위한 기능 및 보안 요구사항

Capabilities and Security Requirements for Network Moving Target Defense Service

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 사이버보안 프로젝트그룹(PG503)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	우사무엘	한국전자통신연구원	선임연구원	응용보안/평가인증 프로젝트그룹 위원	
표준 초안 작성자	이주영	한국전자통신연구원	책임연구원	-	
	우사무엘	한국전자통신연구원	선임연구원	-	
	문대성	한국전자통신연구원	책임연구원	-	
	박경민	한국전자통신연구원	연구원		
사무국 담당		TTA		-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx

서 문

1 표준의 목적

이 표준의 목적은 능동적 네트워크 방어 서비스를 위한 기능 및 보안 요구사항을 정의하는 것이다. 이를 위해 능동적 네트워크 방어 서비스의 개념 및 운영 시나리오를 소개하고, 능동적 네트워크 방어 서비스 설계 시 고려해야 하는 기능 및 보안 요구사항을 정의한다.

2 주요 내용 요약

이 표준은 네트워크 능동적 네트워크 방어 서비스를 설계하는 과정에 고려해야 할 기능 및 보안 요구사항을 정의한다. 이를 위해 먼저 능동적 네트워크 방어 체계의 이해를 돕기 위하여 개념 및 서비스 구성요소들을 소개하고, 이를 기반으로 능동적 네트워크 방어 서비스를 위한 기능 및 보안 요구사항을 정의한다. 본 표준에서 정의한 기능 및 보안 요구사항은 능동적 네트워크 방어 서비스를 개발하는 과정에서 설계 지침서로 활용될 수 있다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

해당사항 없음

3.2 인용 표준과 본 표준의 비교표

해당사항 없음

Preface

1 Purpose

The purpose of this standard is to define capabilities and security requirements for Network Moving Target Defense (Network-MTD) service. It introduces Network-MTD technology and defines capabilities and security requirements to be considered when designing the Network-MTD service.

2 Summary

This standard defines capabilities and security requirements to be considered when designing a Network-MTD service. It analyzes the characteristics of Network-MTD technology to define the capabilities and security requirements. It can be used as a design guide in the process of developing Network-MTD service.

3 Relationship to Reference Standards

None

목 차

능동적 네트워크 방어 서비스를 위한 기능 및 보안 요구사항 (Capabilities and Security Requirements for Network Moving Target Defense Service)

1 적용 범위

본 표준은 능동적 네트워크 방어 서비스를 설계할 때 고려되어야 할 보안 요구사항을 정의하고 있다. 본 표준의 적용 범위는 서비스를 개발하는 주체가 설계 단계에서 지침서로 활용할 수 있도록 참고할 수 있는 서비스 기능 및 보안 요구사항이다. 요구사항 지침과 더불어 능동적 네트워크 방어 서비스의 이해를 돕기 위해, 능동적 네트워크 방어 기술의 개념과 서비스 구성요소에 기반한 서비스 모델에 대한 소개를 포함한다.

2 인용 표준

해당 사항 없음

3 용어 정의

3.1 능동적 사이버 방어 체계(Moving Target Defense)

공격자가 취약점을 악용하기 위해 공격 목표로 삼는 다양한 시스템의 속성들을 공격자의 시선에서는 랜덤하게 보이도록 변화시킴으로써 공격자를 혼란시킴과 동시에 공격 전개를 억제시키는 보안 개념으로서, 변화 대상이 되는 시스템 속성들은 네트워크 속성, 메모리 주소, 실행환경 속성, 소스코드, 데이터 위치 등으로 분류됨

3.2 능동적 네트워크 방어 체계(Network Moving Target Defense)

능동적 사이버 방어 체계에서 네트워크 속성에 해당하는 방어 기술로서, 네트워크를 통한 공격자의 보호대상 호스트 침투 및 취약점 악용에 대하여, 보호대상 호스트의 네트워크 속성을 무작위로 변경시키면서 공격자의 정찰 및 취약점 분석 등의 행위를 사전에 무력화시키기 위한 사이버 방어 기술 개념

3.3 Advanced Persistent Threat(APT) [출처] TTA 정보통신용어사전

특정 공격 대상을 겨냥해 지능적, 지속적으로 은밀하게 공격을 행함으로써 기밀 정보 및 중요 정보를 유출하고 내부 시스템에 피해를 유발하는 해킹 기법으로, 해킹 공격 방법에 제약을 가지지 않는다는 특징을 가짐

3.4 사이버 킬 체인(Cyber Kill Chain)

사이버 킬 체인(Cyber Kill Chain)은 공격자가 특정 조직을 공격할 때 수행하는 공격 행위를 7개의 단계로 정의한 모델이다. 사이버 킬 체인의 7단계는 1. 정찰(Reconnaissance) 2. 공격코드 제작(Weaponization) 3. 전달(Delivery) 4. 취약점 공격(Exploitation) 5. 설치(Installation) 6. 명령 및 제어(Command and Control) 7. 목표 달성(Actions on objectives) 등이다. 사이버 킬 체인은 지능형 위협 공격(APT)을 설명하는데 주로 사용되는 용어임

3.5 단 방향 해시 함수(One way Hash Function) [출처] TTA 정보통신용어사전

SHA-1과 같이 주어진 원문(原文)에서 고정된 길이의 의사난수(疑似亂數)를 생성하는 함수로, 생성된 값은 '해시값'이라고 한다. 불가역적(不可逆的)인 단방향함수를 포함하고 있어서 해시값에서 원문을 재현할 수는 없으며, 같은 해시값을 가진 다른 데이터를 작성하는 것도 극히 어려운 특성이 있음

3.6 투명성(Transparency)

특정 기술이 어떤 시스템 계층에 투명성을 보장한다는 것은, 기술의 적용으로 인한 시스템 수정이나 재구성, 재시작 등이 전혀 필요 없음을 의미함

3.7 공격 접점(Attack surface)

공격자가 정찰을 통해 획득하게 되는 네트워크 호스트의 규모를 지칭하며, 공격 접점이 크거나 넓다는 것은 공격을 당하면 치명적인 노드가 많다는 의미가 아니라, 공격자가 공격 대상을 특정짓기 위해 분석해야 할 대상이 많음을 의미함

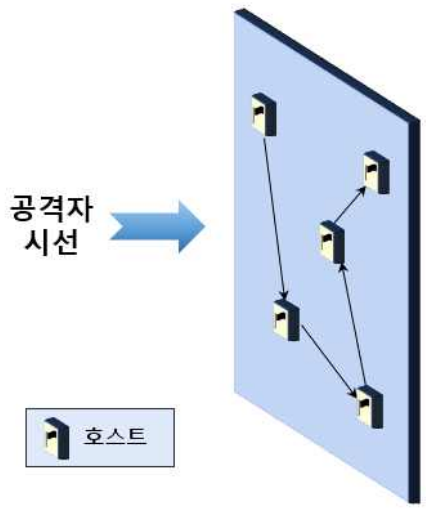
4 약어

MTD	Moving Target Defense
NMTD	Network Moving Target Defense
HAM	Host Address Mutation
NTM	Network Topology Mutation
GRC	General Requirements for service Capabilities
GRS	General Requirement for Security

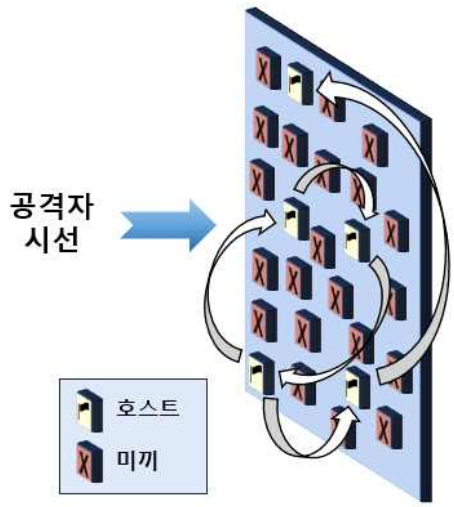
5 능동적 네트워크 방어 체계

5.1 개념

능동적 네트워크 방어 체계는 네트워크를 통해 전개되는 사이버 공격에 대응하기 위하여 네트워크 종단에 위치하는 호스트의 IP주소와 서비스 Port 번호를 지속해서 변화시킴과 동시에 미끼 노드들은 운영하는 것을 기반으로 하는 보안 기술 개념이다. 능동적 네트워크 방어 체계의 목표는 사이버 킬 체인의 전개를 단절시키고 혼란을 주기 위하여, 네트워크를 통해 공격자에게 보이는 공격 대상 호스트의 정보들을 비고정적이고, 비결정적으로 만드는 것이고, 궁극적으로는 공격에 드는 비용을 증가시키는 것이다. 능동적 네트워크 방어 체계는 호스트 주소 변이 기술과 토폴로지 변이 기술로 구성된다. (그림 5-1)과 (그림 5-2)는 공격자가 바라보는 시선에서 각 기술이 주는 효과를 도식화한 것이다.



(그림 5-1) 호스트 주소 변이 기술 효과



(그림 5-2) 토폴로지 변이 기술 효과

호스트 주소 변이 기술은 공격자가 사이버 킬 체인의 첫 단계인 정찰 단계에서 네트워크 스캐닝을 통해 인식한 공격 대상 호스트의 IP/Port 정보를 바꿈으로써, 킬 체인 세 번째 단계인 전달 단계에서 공격 대상이 사라지게 만드는 효과를 준다. 호스트 주소 변이 기술은 이와 같은 개념으로 사이버 킬 체인의 전 구간을 단절시키고, 공격자로 하여금 다음 단계에서 발견되는 호스트들이 최초 공격 대상으로 인식했던 호스트인지 확신할 수 없게끔 혼란을 주게 된다. 호스트 주소 변이 기술을 기반으로 하는 보안 서비스 설계에서 중요하게 고려되어야 할 점은, 호스트의 IP와 서비스 Port가 변화됨에도 불구하고 정상적인 네트워크 서비스 연결은 장애 없이 유지되어야 하며, 이를 위해서는 공격자와 정상적인 사용자를 구분하기 위한 참여자 관리, 참여자들 간의 끊김 없는 네트워크 연결 관리가 요구된다. 추가적으로 호스트 주소 변이 기술이 응용 계층과 시스템 계층에 대하

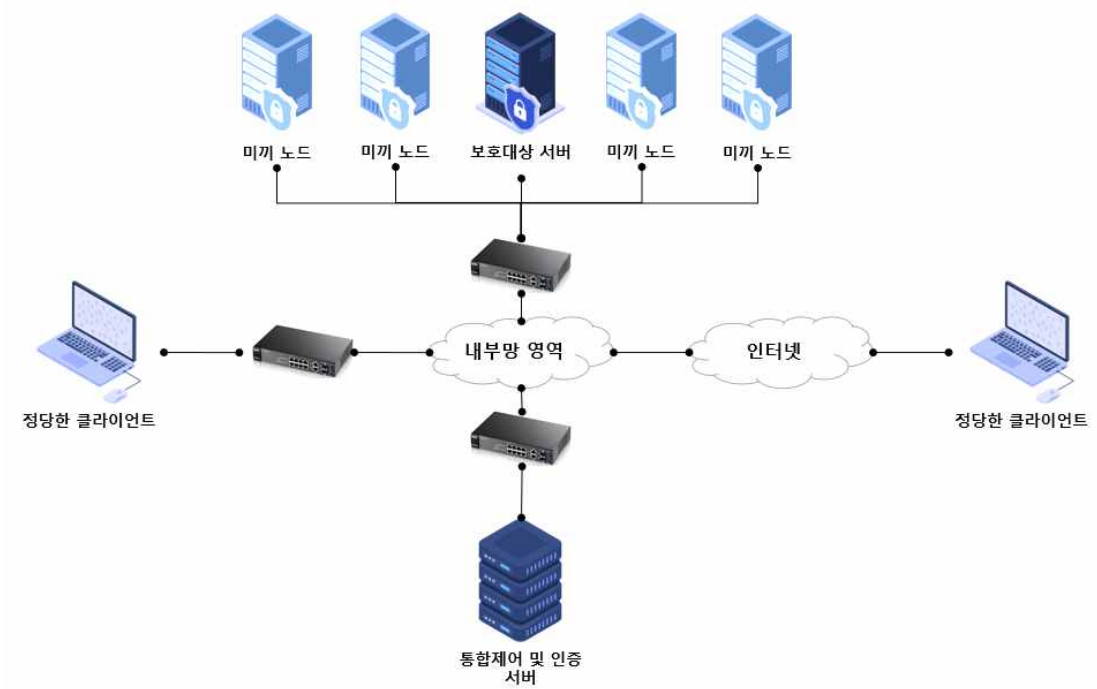
여 투명성(transparency)이 보장된다면 서비스 적용 시 제한사항이 대폭 줄어들 수 있다.

토폴로지 변이 기술은 호스트 주소 변이 기술의 효율을 극대화한다.

공격 대상 네트워크에 1개의 호스트만 존재하여 호스트 주소 변이 기술의 효과가 미약하거나, 공격자의 능력이 매우 숙련되어 있어서 호스트의 주소 변이 주기 이내에 원하는 공격을 성공시킬 수 있는 상황이라면, 토폴로지 변이 기술을 통하여 호스트의 보안을 더욱 강화시킬 수 있다. 토폴로지 변이 기술의 목표는 네트워크 내에 미끼 노드를 여러개 만들어 네트워크 토폴로지가 유동적으로 보이게 함으로써, 공격자에게는 공격 접점(attack surface)이 비약적으로 증가한 것처럼 보이게 하는 것이다. 토폴로지 변이 기술은 독립적으로도 운영될 수도 있으나 궁극적으로는 호스트 주소 변이 기술과 융합되어야만 능동적 네트워크 방어 체계가 완성된다.

5.2 네트워크 개체 관점의 서비스 구성요소

능동적 네트워크 방어 서비스를 운영하기 위한 네트워크 개체 관점에서의 구성요소는 보호대상 서버, 미끼 노드, 정당한 클라이언트, 인증 서버 4가지이다. 보호대상 서버는 능동적 네트워크 방어 서비스를 통해 보호하려는 대상이며 호스트 주소 변이 기술이 수행될 주체이고, 미끼 노드는 공격 접점 확장을 위해 사용되는 실제 또는 가상의 네트워크 노드이며 토폴로지 변이 기술을 통해 운영된다. 본 서비스는 인증 서버를 통해서 보호대상 서버의 서비스를 이용하는 정당한 클라이언트와 그 외의 대상들을 구분해야 한다. (그림 5-3)은 네트워크 엔티티 관점에서의 서비스 구성요소에 대한 한 가지 예시를 도식화한 것이다.

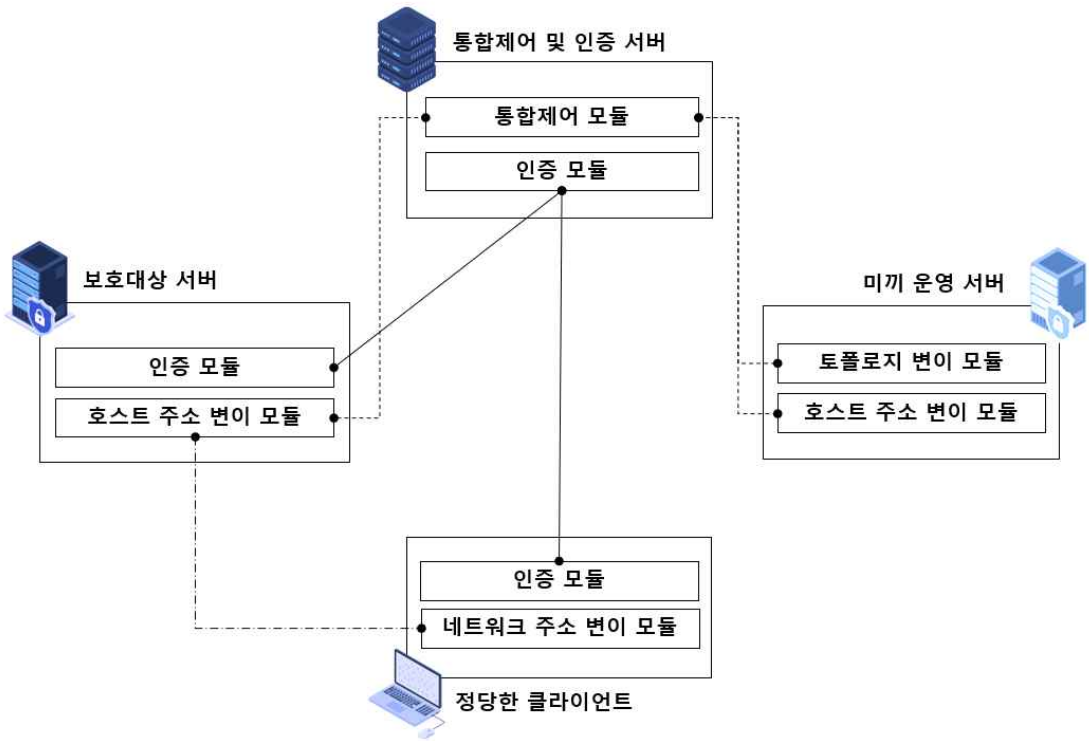


(그림 5-3) 네트워크 엔티티 관점의 서비스 구성요소

(그림 5-3)에서 미끼 노드는 물리적으로 1개의 시스템이 1개의 노드가 될 수도 있으나 자원 효율성 측면에서 가상화 시스템을 이용하는 것이 권장된다. 통합제어 및 인증 서버의 역할은 보호대상 서버와 정당한 클라이언트를 능동적 네트워크 방어 서비스의 참여자로 인증하여 관리하는 것이다. 참여자들끼리만 공유되는 비밀키를 통해 정당한 클라이언트는 보호대상 서버의 호스트 주소 변이 정책을 알 수 있도록 설계되어야 한다. 통합제어 및 인증 서버는 인증 뿐만 아니라 보호대상 서버의 주소 변이 정책을 결정하고 미끼 노드를 제어하기 위한 토폴로지 변이 기술의 정책을 결정하는 역할을 담당한다. 통합제어와 인증을 별도의 시스템으로 분리하여 운영될 수 있다.

5.3 기능 모듈 관점의 서비스 구성요소

네트워크 엔티티 관점의 서비스 구성요소 간의 관계를 기반으로 하는 서비스 기능 간의 관계 예시는 (그림 5-4)와 같다.



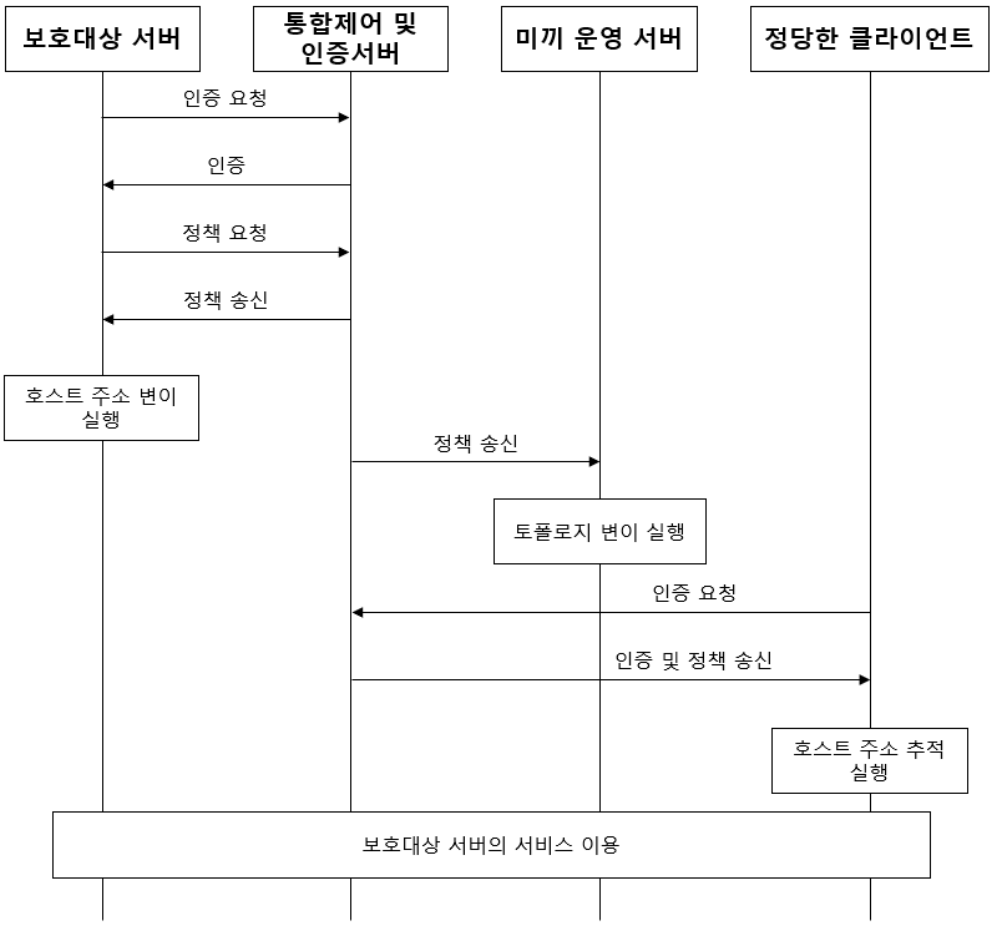
(그림 5-4) 기능 모듈 관점의 서비스 구성요소

서비스 참여자인 보호대상 서버와 정당한 클라이언트는 인증 서버를 통해 서비스 정책을 공유할 수 있는 권한을 얻는다. 보호대상 서버는 통합제어 모듈에서 결정하는 호스트 주소 변이 정책에 기반하여 주소 변이 기능을 실행하게 되고, 인증을 받은 정당한 클라이언트는 통합제어 모듈로부터 보호대상 서버의 정책을 수신하여 보호대상 서버의 바뀌는 IP와 Port를 정당하게 추적할 수 있는 권한을 얻는다. 미끼 운영 서버는 (그림 5-3)에서의 미끼 노드를 가상화 시스템으로 통합 운영하는 시스템을 의미하며, 통합제어 모듈에서 결정하는

미끼 노드의 규모와 속성에 대한 토폴로지 변이 정책을 기반으로 미끼 노드를 운영한다. 미끼 노드는 (그림 5-2)와 같이 호스트 주소 변이 기술과 융합되기 때문에 호스트 주소 변이 정책 동기화를 통해서 미끼 노드와 호스트 간의 주소 충돌을 방지한다. 능동적 네트워크 방어 서비스에서 정당한 클라이언트는 미끼 노드의 존재 여부를 인식하지 않는다. 인증을 통해 정당하게 호스트 주소 변이 정책을 수신한 클라이언트라면 정확하게 보호대상 서버를 추적할 수 있으므로 미끼 노드에 접근하는 상황은 발생하지 않아야 한다.

5.4 서비스 시나리오

능동적 네트워크 방어 서비스의 정상적인 운영 시나리오는 보호대상 서버가 호스트 주소 변이 기술을 실행시키기 위해 인증을 받고 정책을 수신하는 단계를 시작으로 하여 궁극적으로는 주소 변이 정책에 기반한 주소 충돌 없는 미끼 노드 운영, 그리고 정당한 클라이언트가 지속적으로 보호대상 서버와의 연결을 유지해나가는 것이다. 각 구성요소 간의 관계를 기반으로 하는 서비스 시나리오의 순차적 흐름은 (그림 5-5)와 같다.



(그림 5-5) 서비스 시나리오

시나리오의 큰 흐름은 첫 번째로 보호대상 서버가 유효한 정책을 기반으로 호스트 주소 변이 기술을 실행하는 것이고, 두 번째는 미끼 운영 서버가 동일한 정책을 기반으로 토폴

로지 변이 기술을 실행하는 것이다. 미끼 운영 서버는 정책을 기반으로 보호대상 서버가 특정 시간대에 점유하고 있는 IP주소를 알 수 있으므로, 주소 충돌이 발생하지 않도록 미끼 노드 운영이 가능하다. 서비스 관리자의 판단에 따라, 시스템 자원이 가용한 범위 내에서 보호대상 서버가 점유하고 있지 않은 IP주소들에 다수의 미끼 노드를 운영해야 한다. 마지막으로 정당한 클라이언트가 인증 서버를 통해 인증 및 정책을 수신하여 정책을 기반으로 보호대상 서버의 주소를 추적하기 위한 기능을 수행하여 정상적으로 보호대상 서버의 서비스를 제공받는다.

5.5 호스트 주소 변이 정책

호스트 주소 변이는 정책에 기반하며 정책은 시간 단위로 정의되는 특정 라이프타임 구간 내에서 일련의 규칙에 따라 주소를 생성할 수 있도록 구성되어야 한다. (그림 5-6)은 JSON 포맷으로 호스트 주소 변이 정책에 대한 예시를 보여준다. 정책은 도메인의 특성과 관리 방법에 따라 다양하게 구성될 수 있으므로 본 표준에서 정책을 규정하지는 않고, 이와 같이 예시를 통해 운영 방법에 대한 가이드만을 소개한다.

```
{
  “Policy”: {
    “id”: “1”,
    “name”: “server.com",
    "networkSpace": "172.31.0.0/24",
    "timeSyncBasis": 0,
    "mutationInterval": 10,
    “numberOfServices": 2,
    "ports": [
      {
        "port": "22",
        "service": "sshd"
      },
      {
        "port": "80",
        "service": "http"
      }
    ],
    "ipMutationRange": {
      "start": "2",
      "end": "150"
    },
    "lifetime": 86400
  }
}
```

(그림 5-6) 호스트 주소 변이 정책

정책에서 각 속성에 대한 설명은 다음의 <표 5-1>과 같다.

<표 5-1> 호스트 주소 변이 정책 구성

속성	설명
id	서버의 고유 별자, 도메인 name이 없는 서버를 고려함
name	서버의 도메인 name
networkSpace	서버가 속해 있는 네트워크 주소 대역
timeSyncBasis	서버와 클라이언트 간의 주소 논리적시간 동기화를 위한 기본 값
numberOfServices	Port 변이가 수행되는 서비스의 개수
ports	Port 주소 변이를 시킬 서버의 네트워크 서비스 이름과 Port 번호 mapping 정보의 배열
port	Port 변이 대상이 되는 서비스의 원본 Port 번호
service	서비스 이름
ipMutationRange	networkSpace에서 이 서버가 사용할 IP주소 범위
start	IP주소 변이 범위의 시작
end	IP주소 변이 범위의 끝, start가 2고 end가 150이면, 이 서버는 172.31.0.2~172.31.0.150 사이에서만 주소 변이를 수행
lifetime	해당 정책의 유효 기간

6 능동적 네트워크 방어 서비스를 위한 기능 요구사항

6.1 호스트 주소 변이 서비스를 위한 기능 요구사항

호스트 주소 변이 서비스를 위해서는 보호대상 서버가 사용할 익명 주소(IP, Port)를 생성하고, 보호대상 서버에게 서비스를 받아야 하는 정당한 클라이언트들이 보호대상 서버와 동일한 익명 주소를 생성할 수 있는 방법이 필요하다. 보호대상이 위치하고 있는 네트워크에는 하나 이상의 호스트가 존재할 수 있다. 이 경우, 네트워크 안에서는 보호대상 간의 호스트 주소의 충돌이 발생되지 않도록 익명 주소를 생성해야하며, 생성된 주소는 이미 사용 중인 호스트 주소와의 충돌이 없어야 한다.

또한, 호스트 주소의 변경으로 인한 보호대상 서버와 클라이언트 간의 서비스 단절이 발생하지 않도록 별도의 연결 관리 기능이 필요하다. 이를 위해서, 호스트 주소 변이 서비스를 위해서는 익명 주소 생성, 충돌 회피 및 동기화, 네트워크 연결 유지 기능이 필요하며 이에 따라 다음과 같은 기능 요구사항들을 정의한다.

<표 6-1> 호스트 주소 변이 서비스 기능 요구사항

구분	기능 요구사항
GRC-HAM-001	**익명 주소 생성 기능** : 호스트 주소 변이 서비스를 이용하는 개체 간의 상호통신 없이 호스트 주소를 생성하고, 정당한 클라이언트는 보호대상 호스트의 주소를 확인하는 기능
GRC-HAM-002	**익명 주소 충돌 회피 기능** : 특정 시점에 동일한 네트워크 안에서 하나 이상의 호스트가 동일한 익명 주소를 사용하는 것을 방지하는 기능
GRC-HAM-003	**논리적 시간 동기화 기능** : 보호대상 서버의 주소는 일정 시간 주기 단위로 바뀌므로, 서버와 정당한 클라이언트 운영체제의 시간 오차가 존재하는 경우 시간 차이를 극복하기 위한 논리적 시간 동기화 기능
GRC-HAM-004	**네트워크 연결 유지 기능** : 호스트 주소 변경으로 인한 네트워크 연결 장애를 방지하기 위해 보호대상 서버가 호스트 주소를 변경할 때, 이전 주소로 맺어진 네트워크 연결을 재구성 없이 유지 또는 이전시키는 기능

* GRC: General Requirements for service Capabilities

6.2 토폴로지 변이 서비스를 위한 기능 요구사항

토폴로지 변이 서비스는 공격자가 정확한 네트워크 호스트 정보를 확인하기 어렵도록 네트워크에 미끼 노드를 생성, 배치, 운용한다. 고정된 정책에 따라 미끼 노드를 생성하고 배치하면 숙련된 공격자에 의해 짧은 시간 안에 필터링 될 수 있으므로 미끼 노드의 구성도 지속적으로 변경해야 한다. 미끼 노드 구성 정책은 운영체제, Port로 접근 가능한 네트워크 서비스를 바꾸는 목적으로 구성된다. 토폴로지 변이 서비스의 대전제는 정당한 클라이언트는 미끼 노드에 접근하지 않는다는 것이므로, 만약 미끼 노드로의 연결 시도가 있었다면 일차적으로 공격 행위로 간주하게 된다. 마지막으로 미끼 운영 서버는 가상화 시스템을 기반으로 다수의 미끼 노드를 생성하게 되는데, 시스템 자원 관리가 이루어지지 않으면, 미끼 노드가 많아지는 대신 정교한 스캐닝에 대해서는 응답시간 지연 폭이 커짐으로써 공격자에게 쉽게 필터링 될 수 있다. 이러한 요소들을 종합하여 미끼 노드 생성, 운용 관리 및 침입 탐지 역할에 따라 다음과 같은 기능 요구사항들을 정의한다.

<표 6-2> 토폴로지 변이 서비스 기능 요구사항

구분	기능 요구사항
GRC-NTM-001	**미끼 노드 생성 기능** : 가상의 미끼 노드를 생성해 네트워크 보호대상 호스트가 점유하지 않은 IP주소를 할당하는 기능
GRC-NTM-002	**미끼 노드 주소 변경 기능** : 보호대상 호스트가 주소를 바꾸기 직전에 바뀔 IP주소를 점유하고 있는 미끼 노드의 IP주소를 보호대상 호스트의 이전 IP주소로 변경하는 기능 : 호스트 주소 변이 정책의 시간 주기에 맞춰서 모든 미끼 노드들이 중복되지 않는 IP주소를 할당받아 전체 주소를 바꾸는 기능
GRC-NTM-003	**미끼 노드 구성 변경 기능** : 미끼 노드의 구성요소인 운영체제, 네트워크 서비스를 임의의 랜덤한 속성으로 교체하는 기능
GRC-NTM-004	**비정상 행위 수집 및 보고 기능** : 미끼 노드로 들어오는 모든 패킷 및 접속 시도에 대한 로그를 수집하여 비정상 행위 처리 기능을 담당하는 3rd 시스템으로 보고하는 기능
GRC-NTM-005	**시스템 자원 관리 기능** : 미끼 노드의 패킷 응답시간이 일정수준 이하로 떨어지지 않도록 토폴로지 변이를 통한 공격 접정 확장의 규모를 동적 관리하는 기능

7 능동적 네트워크 방어 서비스를 위한 보안 요구사항

본 장에서는 능동적 네트워크 방어 체계 관련 기존 기술들의 한계점을 기반으로 서비스를 운용할 때 고려해야 하는 보안 요구사항들을 정의한다.

<표 7-1> 능동적 네트워크 방어 서비스 보안 요구사항

구분	보안 요구사항
GRS-NMTD-001	미끼 노드 감염 대응
GRS-NMTD-002	서비스 참여 개체 인증
GRS-NMTD-003	호스트 주소 생성용 키 관리

7.1 미끼 노드 감염 대응

토폴로지 변이 서비스는 공격 접점을 확장시키기 때문에 보호대상 호스트가 아니더라도 미끼 노드가 무작위 공격에 의해서 공격자에게 점유될 수가 있다. 미끼 노드는 보호대상 호스트와 동일 네트워크에 존재하거나 미끼 운영 서버 가상 시스템의 일부 파티션일 수 있기 때문에, 미끼 노드가 감염됨으로 인해 발생하는 보안 위협에 대한 대응이 필요하다. 미끼 노드는 보호대상 서버처럼 서비스를 제공하는 역할은 수행하지 않기 때문에 외부 노드들과의 상호작용을 제한시켜도 무방하다. 그러므로, 미끼 노드의 감염에 대응하기 위해서는 공격자가 정찰 단계에서 보내는 패킷에 응답만 하되 모든 네트워크 연결 생성 시도는 차단하는 기능이 필요하다. 그럼에도 불구하고 관리 미흡이나 발견되지 않은 취약점들로 인하여 미끼 노드가 감염되는 상황에 대비하기 위하여, 미끼 운영 서버의 가상 시스템에 존재하는 네트워크 브릿지는 미끼 노드로부터 자발적으로 빠져나오려고 하는 패킷을 차단하는 정책이 적용되어야 한다. 즉, 미끼 노드가 공격당했을지라도, 노드 내에서 이루어지는 공격 행위가 외부로 빠져나가지 못하도록 하기 위한 보안 대책이 있어야만 한다.

7.2 서비스 참여 개체 인증

개체 인증은 보호대상 호스트와 정당한 클라이언트를 확인하는 과정으로, 개체 인증을 통해 정당한 개체들만이 능동적 네트워크 방어 서비스를 이용할 수 있어야 한다. 호스트 주소 변이를 사용하는 보호대상 서버들과 서비스를 제공받는 정당한 클라이언트들이 인증의 대상이며, 인증을 통과한 정당한 개체들만 지속적으로 변경되는 호스트 주소를 계속해서 알 수 있어야 한다.

일반적으로 인증 기법은 개체의 정당성만 확인하는 단방향 인증과 보호대상 호스트와 클라이언트가 서로를 인증하는 양방향 인증으로 분류된다. 또한, 인증에 사용되는 암호학적

기법의 특징에 따라 대칭키 기반의 인증 기법과 공개키 기반의 인증기법으로 나뉜다.

능동적 네트워크 방어 서비스를 위해 사용되는 인증 기법을 본 표준에서 한정하지는 않으며, <표 7-2>에 제시된 개체 인증 관련 ISO/IEC 표준을 참고하여 기존 정보통신 환경에서 사용되고 있는 인증 기법들 중 안전성이 증명된 인증 기법을 사용하는 것을 권장한다.

<표 7-2> 개체 인증 표준 분류

구분		인증 기법
대칭키 기반 인증 표준	단방향인증	(1) ISO/IEC 9798-2 one-pass unilateral
		(2) ISO/IEC 9798-2 two-pass unilateral
	양방향인증	(3) ISO/IEC 9798-2 two-pass mutual
		(4) ISO/IEC 9798-2 three-pass mutual
공개키 기반 인증 표준	단방향인증	(5) ISO/IEC 9798-3 one-pass unilateral
		(6) ISO/IEC 9798-3 two-pass unilateral
	양방향인증	(7) ISO/IEC 9798-3 two-pass mutual
		(8) ISO/IEC 9798-3 three-pass mutual
		(9) ISO/IEC 9798-3 two-pass parallel

7.3. 호스트 주소 생성용 키관리

호스트 주소 변이 서비스에서 보호대상 호스트가 새로운 주소를 생성하고, 정당한 클라이언트가 보호대상 호스트의 주소를 알아내기 위해서는 다음과 같은 두 가지 방법을 사용할 수 있다.

(1) 서비스 도메인의 인증서버와 같은 trusted party가 클라이언트에게 보호대상 호스트의 호스트 주소를 전달하는 방법

(2) 클라이언트가 보호대상 호스트의 주소를 생성하기 위해, trusted party로부터 사용되는 비밀키를 전달받고, 이후 클라이언트 스스로 보호대상 호스트의 주소를 직접 생성하는 방법

첫 번째 방법의 경우, 주소가 바뀔 때마다 안전하게 호스트 주소를 공유하는 방법이 필수적으로 제공되어야 하고, 바뀐 주소의 적용 시점에 대한 동기화가 필요하다.

두 번째 방법에서는 호스트 주소 변이 서비스에서는 보호대상 호스트의 주소 변경 시,

새로운 주소를 생성하기 위해 비밀키를 사용할 수 있다. 이 때, 호스트 주소 변이 서비스를 사용하는 모든 개체들은 7.2절에서 기술한 개체 인증 과정을 통해 정당한 사용자임을 확인하고 비밀키를 발급받아 사용해야 한다.

비밀키를 사용하는 경우에는, 호스트 주소 변이에 사용할 익명 주소를 생성하기 위해 사용하는 키 분배, 업데이트, 폐기하기 위한 키 관리가 필요하다. 발급된 키는 유효한 사용자만이 알 수 있도록 관리되어야 하며, 악의적인 사용자가 해당 키를 알게 된다면, 호스트 주소 변이 서비스에 의한 보호 기능이 정상적으로 작동할 수 없다. 또한, 효율적인 키 관리를 위해서는 호스트 주소 변이 기술이 적용될 도메인의 특징에 따라 적합한 키 관리 기법을 사용해야 한다. 키 관리는 기존의 기법들 중 안전한 기법을 선택적으로 사용할 수 있고, 기존 표준을 따를 수 있다.

부 속 서 A

(본 부속서는 표준 내용의 일부임)

해당 사항 없음

부 록 I

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

해당 사항 없음

부 록 II-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

해당 사항 없음

부 록 II-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

해당 사항 없음

부 록 II-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

해당 사항 없음

부 록 II-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

해당 사항 없음

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 II-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 II-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
			- 표준문서 양식을 준수 - “MTD” -> “능동형 방어 기술” - “NMTD” -> “능동형 네트워크 방어 기술 - 5장 기존 내용을 논문 형식이 아닌 일반적인 기술 설명으로 대체 - 요구사항 정의가 서술형으로 된 부분을 표로 구성	PG503