SDN 기반 동적 네트워크 은닉 기술 (SDN-based Technologies for Moving Target Defense)

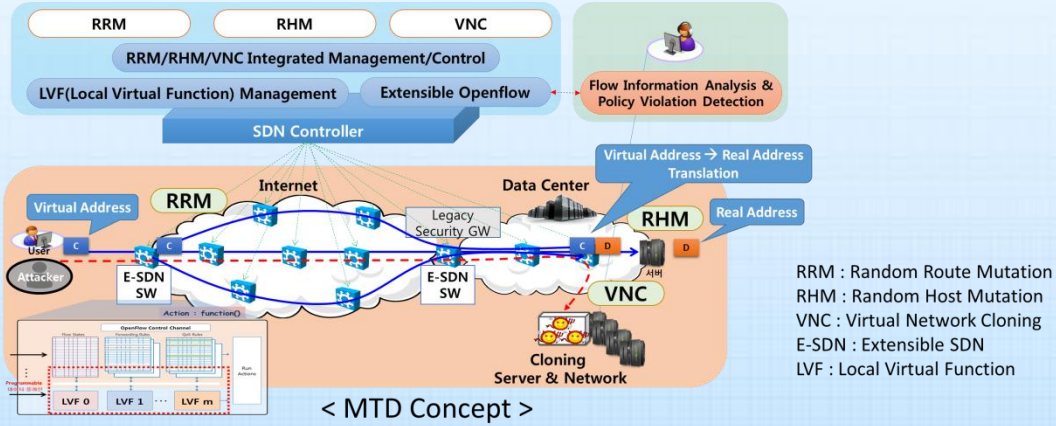
신뢰네트워킹연구실

고 남 석

ETRI
Electronics and Telecommunications Research Institute

CONTENTS

기술 개요(1)-영문

SDN-based Technologies for Moving Target Defense Namseok Ko (nsko@etri.re.kr)			
SDN-based Technologies for Moving Target Defense Network Protection			
Concept	• Network protection technologies which make systems dynamic and therefore harder to explore and predict by constantly changing IP addresses of systems (random host mutation or RHM) and/or routes to the systems (random route mutation or RRM) • Dynamic decoy network cloning technology (VNC) which work interworking with RRM and RHM  < MTD Concept >		

Service Offering	• Network and system protection from network threats including APT for various networks
	  • Special purpose networks such as banking networks and medical networks,
	  • Enterprise networks, cloud networks		

Comparative Advantages	• **Decrease attacking probability** by constantly changing the route to systems • Forbid **backtracking** by hiding real IP addresses to systems • SDN-based **detecting/blocking/detouring of suspicious traffic**		
Patents (Domestic)	Application(O) / Registration( )	Patents (International)	Application( ) / Registration( )

기술 개요(2)

1. 기술개발의 필요성

- **고객 및 시장의 니즈**
  - 기존 경계 기반 네트워크 보안 체계가 한계에 직면하여, 네트워크 기술 기반 변혁적인 R&D 필요
  - **동적 경로 제어** : 네트워크 경로가 고정되면 도·감청 및 공격에 취약하므로 주기적인 경로 변경을 통해 경로 기밀성을 제공하는 기술 필요
  - **호스트 은닉** : 정적 IP 주소를 기반으로 하는 인터넷 서비스는 공격자들이 네트워크를 스캔하여 정확하고 신속하게 목표물을 설정 및 공격하는데 상당히 취약하므로 이에 대한 대응책 필요
  - **네트워크 클로닝** : APT 등 다양한 위협 요소로부터 네트워크를 방어하기 위해 차단 기술보다 "유인 후 분석 차단"방어 전략의 필요성 증대

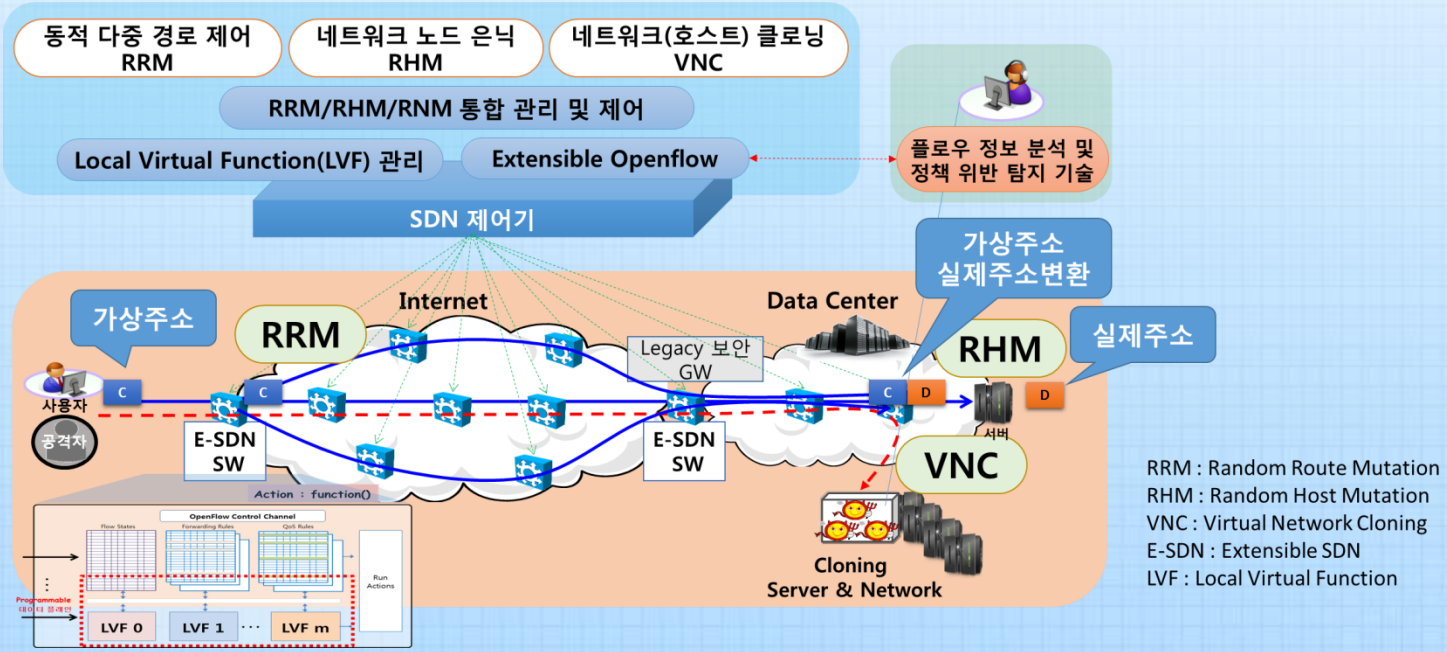
기술 개요(3)

2. 기술의 개념 및 구성

기술의 개념

- SDN 기반으로 **네트워크 구성을 동적으로 변경하여** 악의적 사용자의 공격에 대한 **예측불가능성(Unpredictability)**, **불확정성(Uncertainty)** 및 **비용(Cost)**을 증가시켜 취약점 노출을 어렵게 만드는 **네트워크 보호 기술**

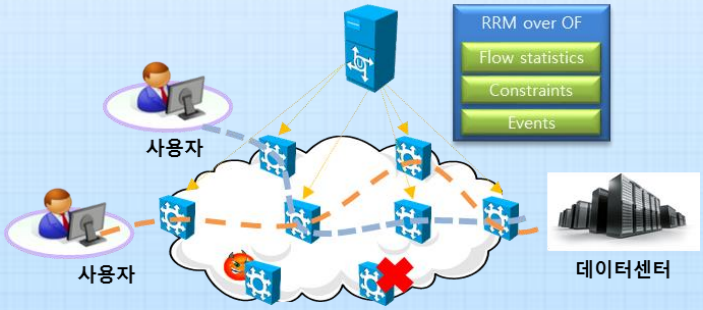
기술의 구성도



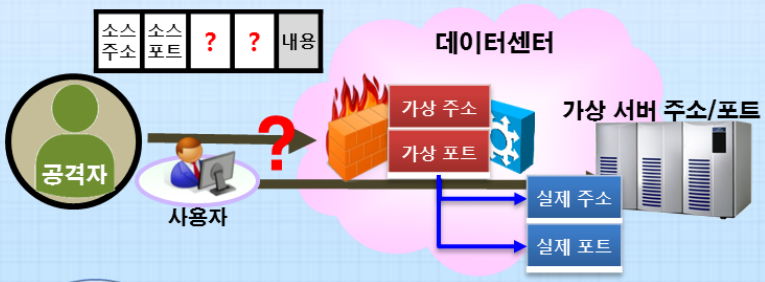
개발기술의 주요내용(1)

1. 기술의 특징

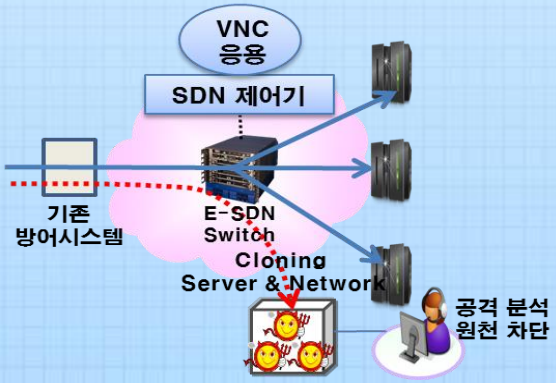
- **고객/시장의 니즈를 충족**
  - 기존 경계 기반 네트워크 보안 개념을 벗어나, 공격자의 타겟인 서버, 서버로 구성된 네트워크, 그리고 서버로의 경로를 동적으로 은닉시키는 변혁적 기술
- **기술의 상세 사양**
  - 동적 다중 경로 제어 기술



  - 네트워크 노드 은닉 기술



  - 가상 네트워크 은닉 기술



개발기술의 주요내용(2)

2. 경쟁기술대비 우수성

- **경쟁기술/대체기술 현황**
  - 동적 다중경로 제어 기술은 현재 학계 연구 수준으로, North Carolina 대학의 연구결과에 따르면 SMT(Satisfiability Modulo Theories) Solver를 이용한 다중경로 생성기술이 연구되고 있음
  - 네트워크 노드 은닉 기술 역시 학계 연구 수준으로, OF-RHM(Openflow Random Host Mutation) 연구결과에 따르면 SDN기반의 IP 주소 변경을 통한 노드 은닉 기술의 가능성을 제시함
  - 미국 국책 연구기관인 ORNL(Oak Ridge National Laboratory)에서 2009년부터 2011년까지 사이버 침입 대응 기술로 VM Live-cloning 기술을 개발하였으며 Shadow Network 사를 통해 APT 공격 대응 장비 기술로 발전시키고 있음

개발기술의 주요내용(2)

2. 경쟁기술대비 우수성

- 경쟁기술/대체기술 대비 우수한 점

경쟁기술	본 기술의 우수성
Efficient RRM 기술 (University of North Carolina)	• 네트워크 규모의 확장성 및 경로계산시간을 고려한 저복잡도 경로계산 알고리즘 적용을 통한 성능향상 (100 router환경에서 1s → 114ms) • 다중경로 생성시 사전경로 생성과 반응경로 생성으로 구분하여, 네트워크 이벤트(ex. Link Failure) 발생시에도 동작 가능
OF-RHM 기술 (University of North Carolina)	• Hash chain을 이용한 IP, 포트 생성을 통해 역추적 방지 기능 제공 및 속도향상 • RHM의 파라미터(변경주기, 재사용주기) 추가를 통한 효율성 향상
Dynamic Honeypot 기술	• 서비스를 제공하는 서버를 은닉시키고, 서버까지의 경로를 은닉시킴으로써, 공격 확률을 이중 삼중으로 낮출 수 있음 • SDN 기반으로 의심 트래픽을 탐지할 수 있으며, 단순 차단 뿐만 아니라 격리/추적까지 가능한 구조임

개발기술의 주요내용(3)

3. 기술의 완성도

- **기술개발 완료시기 및 완성도**
  - 기술개발 완료 시기 : 2017년 1월 (완성도 : 80%)
  - 이전 가능 (예상) 시기 : 2017년 3월 (완성도 : 90%)

- **기술이전 범위 및 내용**
  - 동적 다중 경로 설정/제어 기술
    - ✓ Proactive Secure & Survivable RRM 제어 기술
    - ✓ Reactive Secure & Survivable RRM 제어 기술
  - 네트워크 노드 은닉 기술
    - ✓ 가상 IP Pool 관리 및 생성 기술
    - ✓ 가상 IP 할당 및 제어 기술
  - 가상 네트워크 은닉 기술
    - ✓ 서버 클로닝 기술
    - ✓ 정책 위반 탐지 기술

개발기술의 주요내용(4)

4. 표준화 및 특허

표준화 동향

- 미래네트워크보안 표준은 ITU SG13에서 네트워크 보안 요구사항 및 인증 기술의 국제 표준이 제정되었으며, 현재 미래네트워크 환경에서 Mobility Security와 클라우드 컴퓨팅 서비스 보안 프레임워크 국제 표준이 개발되고 있음
- ITU-T SG17은 SDN을 이용한 응용 및 서비스, 유즈케이스 등의 권고안 개발을 Q6/17에서 진행하고 있음

보유 특허

출원/ 등록 구분	특허명	출원국 (등록)	출원(등록)번호	출원(등록) 년도
출원	상황인지 기반 의심 트래픽 대응 장치 및 방법	대한민국	10-2016-0065011	2016.05.26.
출원	동적 네트워크 환경에서의 네트워크 보안 강화 방법 및 장치	대한민국	10-2016-0034211	2016.03.22.

기술적용 분야 및 기술의 시장성(1)

1. 기술이 적용되는 제품/서비스

- **SDN/NFV 기반 보안 솔루션**
  - NFV 프레임워크에 VNF 형태로 적용
  - SDN/NFV 플랫폼에 보안 VNF를 추가함으로써 SDN/NFV 기반 보안 솔루션으로 확대
- **SDN 제어기**
  - Proactive RRM 제어 모듈, Reactive RRM 제어 모듈
  - 기존 SDN 제어기에 망 은닉 응용서비스를 추가
  - 기존 망 앞단에 은닉 네트워크 추가 구성을 통한 보안성 강화
- **가상 서버 클로닝 플랫폼**
  - SDN 제어기와 연동하는 응용 서버로 개발
  - APT 등 다양한 위협 요소로부터 물리 서버를 방어할 수 있어, 금융, 의료 시스템 등에 활용 가능
  - 엔터프라이즈나 데이터 센터 등 주요 지점 네트워크의 방어 장비 및 공격자 탐지 시스템으로 활용 가능

기술적용 분야 및 기술의 시장성(2)

2. 해당 제품/서비스 시장 규모 및 국내외 동향

시장 규모 및 향후 전망

- SDN 보안 응용 제품 시장은 시작 단계이며, 데이터 센터에서 SDN 등을 이용한 가상 보안 장비의 증가 추세를 보이고 있으며, 2012년 이후 5년간 44% 성장 예상 (출처: Infonetics Research)

단위 : 억원

년도	2016년	2018년	2020년
세계 시장 규모	41,371	128,343	244,774
한국 시장 규모	414	1,283	2,448

국내외 주요 사업자 및 시장동향

- Big Switch Network는 60억달러를 투자받아 vArmour라는 보안 제품을 개발하였으며, Flow 단위로 보안 규칙을 설정 기능 제공
- NEC와 Radware는 NEC의 SDN 제어기, ProgrammableFlow와 연동하는 보안 솔루션을 개발하였으며, DDoS 탐지 등의 기능 제공
- HP는 자체 개발한 제어기와 기존의 보안솔루션을 통합 운용할 수 있는 제품을 개발하기 위해 Sentinel 프로젝트를 진행 중
- 국내 SDN 보안 관련 기술은 시작 단계이고, 국산 상용 제품은 전무한 수준임

Ⅳ 기대효과

기술 도입 효과

기술 도입으로 인한 경제적 효과

- 안전한 네트워크 구축을 위한 SDN 기반 장비 개발은 통신장비의 외산종속 탈피 기회를 제공함과 동시에, 장비 국산화를 통한 국내 네트워크 산업 활성화 기회 제공
- 기존 SDN 스위치와의 호환성을 제공하는 동시에 미래 네트워크를 지향하는 신기술로서, 국내 네트워크 관련 업체로의 기술이전을 통해 국내 업체의 기술 경쟁력을 강화하고 국내·외 시장 진출 교두보 마련 가능
- SDN 장비를 상용화하고, 보안성이 중요한 정부·공공기관망을 필두로 시장에 진출, 50%의 국산화를 달성할 경우, 약 6천억 원의 수입대체 효과 기대

기술사업화로 인한 파급효과

- 네트워크 구조 측면에서 안전성 강화 메커니즘을 제공하므로, 현재의 인터넷보다 훨씬 안전하고 효율적인 네트워크 기술의 기반 마련
- 현재 대형 글로벌 벤더 위주의 장비 시장 구조로 야기된 네트워킹/컴퓨팅 장비의 해외 의존성 탈피 및 핵심 시스템 플랫폼 기술 확보