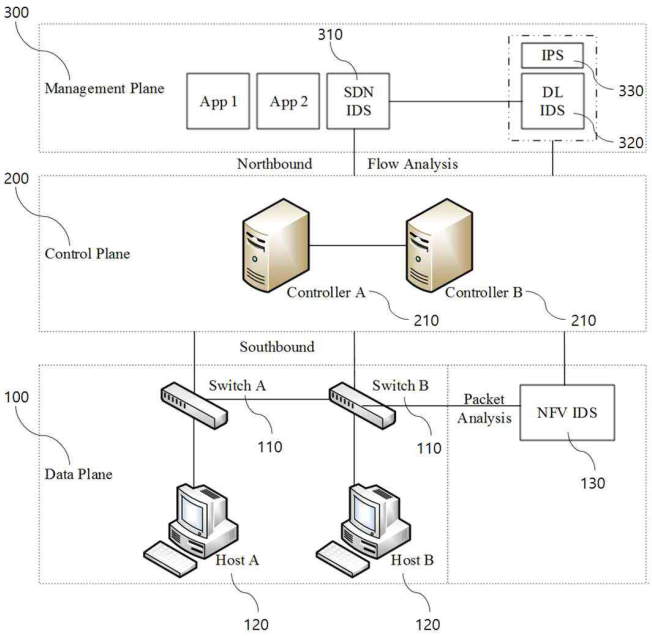
SDN에서의 적응형 보안시스템

The garbage can which classifies the trash



[대상 기술의 SDN에서의 적응형 보안시스템]

발명자	이상곤, 이훈재, 임준휘, 안드리 안토 빈첸시오 크리스티안
출원번호	10-2016-0063910
출원일자	2016-05-25
등록번호	10-1836214 (KR)
등록일자	2018-03-02

기술아젠다

- ✓ 안전한 사회 - 사이버 안전 및 정보보호
- ✓ 스마트한 사회 - 시공간상의 원활한 정보교환

과학기술분류

- ✓ 공통 보안기술(L0301), 서비스/응용보안(L0303), 정보시스템 보안(SC1108)

표준산업분류

- ✓ 시스템 소프트웨어 개발 및 공급업(58221)

신성장동력 • 원천기술분야

- ✓ 차세대SW(소프트웨어) 및 보안 - 융합보안

기술개요 DSU+

- 트래픽을 제어기에게 전달하지 않고 패킷 수준 분석을 네트워크 기능 가상화 IDS에게 전달하여 SDN(software defined network, 소프트웨어 정의 네트워크)의 보안을 관리하는 혼합형 솔루션의 구현 기술임

기존 기술의 문제점

- SDN 제어기는 특정 흐름의 통계를 알고 있으며 메시지의 유형 까지도 알 수 있지만, 트래픽이 악성코드를 포함하고 있는지를 결정하지는 못한다.
- SDN 제어기는 흐름으로 네트워크를 제어하도록 설계되었기 때문에 데이터 평면에 존재하는 보안 문제는 완화시키지 못한다.
- 제어기는 공격을 방어할 수 없으며 패킷 레벨 분석 없이는 어느 호스트가 공격을 착수 했는지 알려주지 못한다.

- 흐름 분석으로 제어 평면에 대한 악성 행위를 추출 할 수 있지만 데이터 평면에 대한 공격분석은 불가능하다.
- 종래의 기술은 흐름제어로 SDN 관리를 시도하였지만 호스트나 스위치를 공격 목표로 하는 Dos 공격과 같은 데이터 평면에 존재하는 보안 위험이 간과되었다. 집적화로 SDN에서 데이터 평면 위협이 가능하지만 제어기에 흐름 관리 트래픽뿐만 아니라 모든 데이터 패킷을 제어기에게 전달하게 되어 네트워크 대역폭 소모가 많으며 제어기에 과중한 부하를 초래하게 된다.
- 결국 이러한 구현은 사우드 바운드(제어기와 스위치 혹은 라우터 장치 간의 채널) 통신에 병목현상을 초래한다.

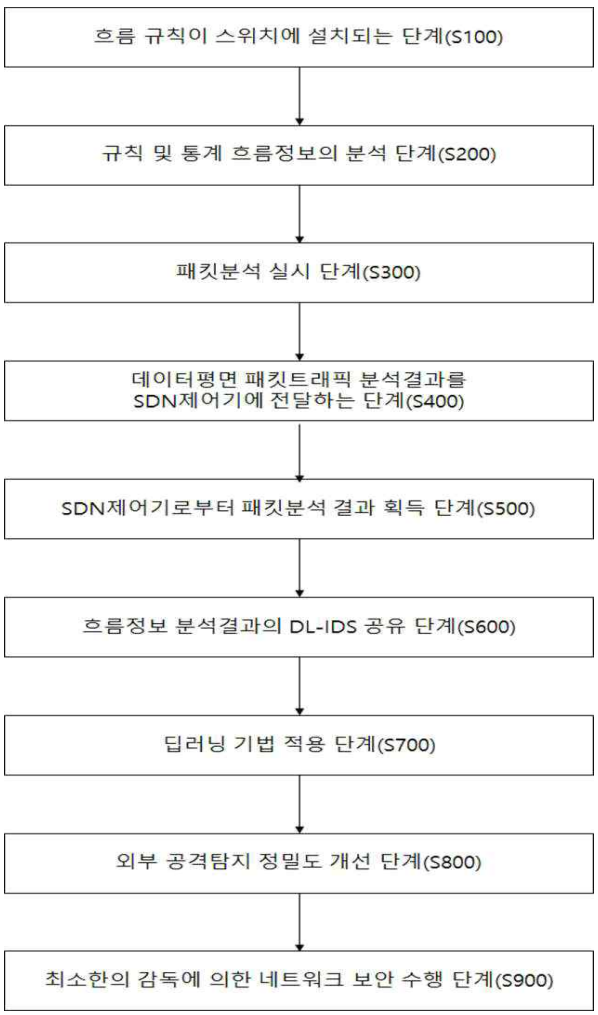
기술의 요지

- 본 발명은 SDN에서의 적응형 보안시스템 및 이의 구동방법에 관한 것으로서, 더욱 상세하게는 모든 트래픽을 제어기에게 전달하지 않고 패킷 수준 분석을 네트워크 기능 가상화 IDS에게 전달하여 SDN 보안을 관리하는 혼합형 솔루션의 구현 기술에 관한 것이다.

개발 기술의 효과

- 모든 트래픽을 제어기에게 전달하지 않고 패킷 수준 분석을 NFV-IDS에게 전달하여 SDN 보안을 관리하는 혼합형 솔루션의 구현 기술을 제공하는 효과가 있다.

대표 도면



[SDN에서의 적응형 보안시스템 구동방법의 실시 흐름도]

기술의 작용

- SDN에서의 적응형 보안시스템에 있어서,
- 데이터평면(100)에 위치하는 스위치(110);
- 상기 스위치(110)에 연결된 호스트(120);
- 네트워크의 구성요소인 하드웨어와 소프트웨어를 분리하고 범용 서비스 가상화 기반에서 네트워크 기능을 가상 화해 제공하는 NFV-IDS(130);
- 제어평면(200)에 위치하고 네트워크 장비의 상기 데이터평면(100)과 상기 제어평면(200)을 분리하고 각 기능을 처리하며 상기 스위치(110) 또는 상기 호스트(120)에서 받은 흐름정보를 이용하여 네트워크 모니터 및 로드 밸런서의 어플리케이션을 운영하는 SDN제어기(210);
- 관리평면(300)에 위치하고 상기 스위치(110) 또는 상기 호스트(120) 중에 악의적인 공격을 수행 중인 것으로 의심되는 것을 색출하기 위한 SDN-IDS(310);
- 상기 SDN-IDS(310)의 신호를 입력받아서, CNN(conventional neural network)과 DBN(deep belief network)가 조합되어 기계학습이 수행되는 DL(deep learning)-IDS(320);
- 상기 스위치(110) 또는 상기 호스트(120) 중에 악의적인 공격을 수행하여 네트워크 시스템에 액세스하는 것을 차단하는 IPS(330)로 구성.

적용 시장 DSU+

- 시스템 소프트웨어 개발 및 공급업(KSIC 58221) 시장 – 컴퓨터 및 서버 등 하드웨어에 설치되는 응용 소프트웨어를 유기적으로 작동시키는 시스템 소프트웨어를 개발·공급하는 산업활동을 말한다. 하드웨어 운영체제(OS) 기능 중 파일 관리, 메모리 관리, 바이러스 예방, 파일 압축 등의 기능을 보완하는 유틸리티 소프트웨어를 개발·공급하는 산업활동도 포함
- 미국은 SW개발 및 공급업(5112) 시장

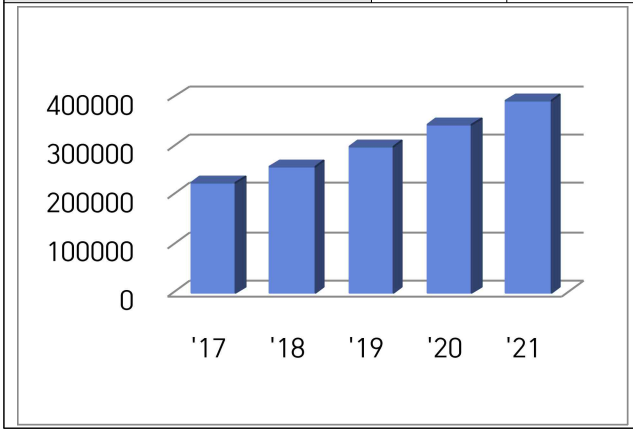
시장 규모

- SW개발 및 공급업(5112)의 미국 시장 규모는 2017년 224,400백만 달러에서 증가(CAGR 15%)되어, 2021년에는 392,300백만 달러에 달할 것으로 예측
- 시스템 소프트웨어 개발 및 공급업(KSIC 58221)의 국내 시장 규모는 2017년 161,840억 원에서 증가(CAGR 2.9%)되어, 2021년에는 181,449억 원에 달할 것으로 예측

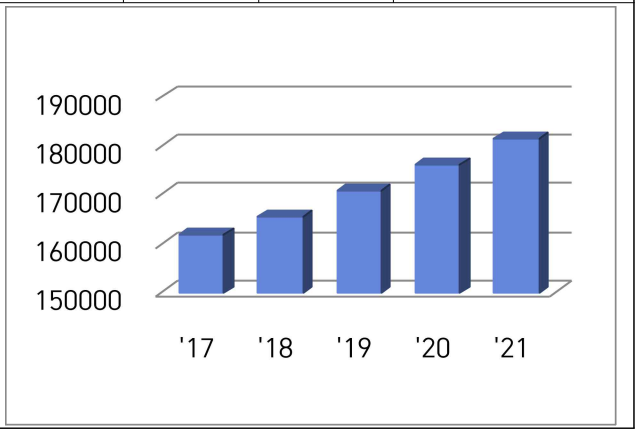
[표] 미국/국내 시스템 소프트웨어 개발 및 공급 분야의 시장규모 추이

단위: 억 원, 백만 달러, %

구분	'17	'18	'19	'20	'21	CAGR(17~21)
미국 시장(백만 달러)	224,400	257,900	296,600	341,100	392,300	15%
국내 시장(억 원)	161,840	165,417	170,761	176,105	181,449	2.9%



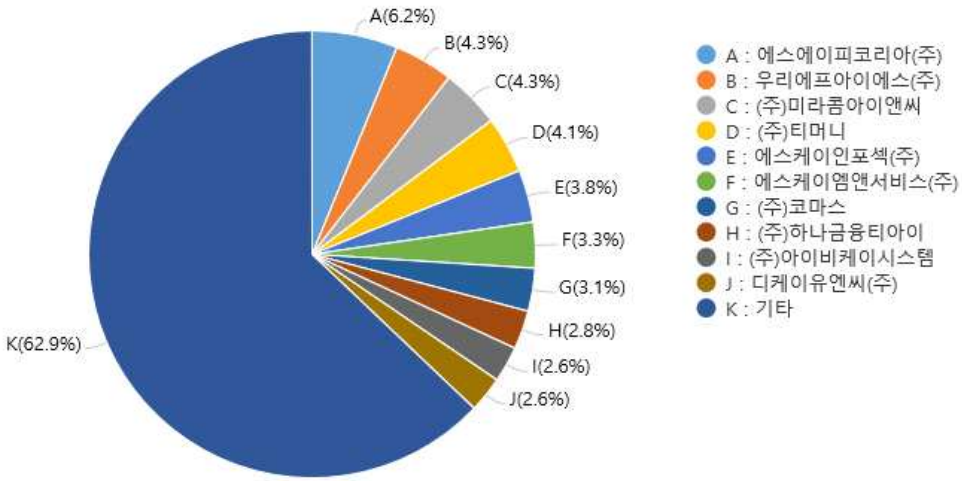
[미국 시장]



[국내 시장]

*출처: 미국 시장은 정보통신정책연구원(2017) 재가공, 국내 시장은 한국과학기술정보연구원(2019)

국내 시장 점유율



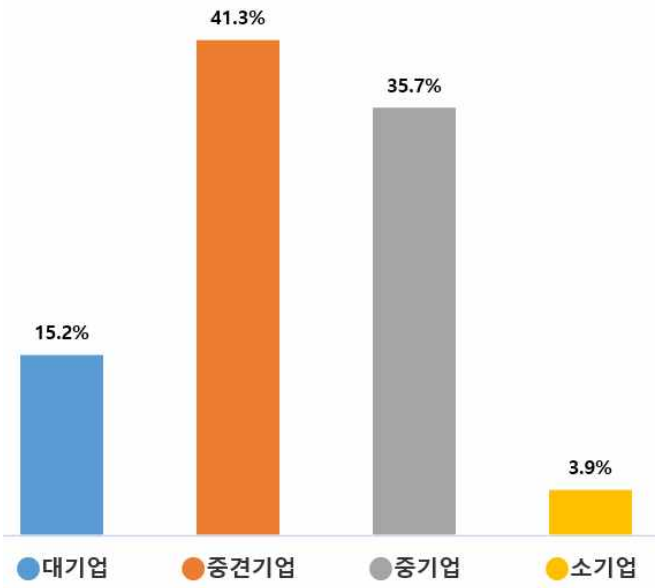
*출처: 한국과학기술정보연구원(2019, 2018년도 기준으로 작성)

시장 집중도

- 기업집중도를 보면, 시스템 소프트웨어 개발 및 공급업(KSIC 58221) 시장에서 허핀달-허쉬만 지수(Herfindahl Hirschman Index, HHI. 시장집중도 측정방법으로 기업의 시장점유율의 제곱을 모두 합산한 지수)가 203이고, 상위 3대 기업 집중도(Concentration Ratio3, CR3. 시장점유율 1~3위 기업의 시장점유율의 합)는 14.8%를 차지하며 중소, 중견기업 매출 비중이 85%를 차지하는 시장으로 집중도가 낮은 시장에 해당함

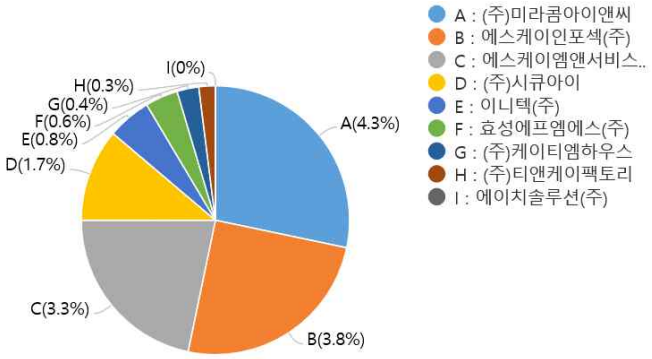
*출처: 한국과학기술정보연구원(2019)

규모별 시장 점유율



*출처: 한국과학기술정보연구원(2019)

대기업 경쟁구조



*출처: 한국과학기술정보연구원(2019)

기술동향 DSU+

- 5G 코어 네트워크에서는 코어와 에지 네트워크의 분리, 네트워크 슬라이싱, 가상화된 NF(Network Function) 기능 등을 제공하기 위해 하드웨어 종속적인 인프라에서 SDN(Software Defined Networking)과 NFV(Network Function Virtualization) 기술을 활용한 소프트웨어 기반 인프라로의 전환이 가속화될 것으로 예상

기술 특징

- 소프트웨어기반 5G 분산 코어 네트워크에서는 SDN 및 NFV 보안 이슈가 중요한 문제로 부각됨
- SDN 네트워크는 네트워크 제어 기능(SDN 컨트롤러)과 트래픽 전달(SDN 스위치) 기능을 분리하여, 하드웨어적으로 구현된 네트워크 전달 기능에 대한 제어를 소프트웨어로 제어하고 통제하기 위한 기술임
- 이에 SDN 컨트롤러와 SDN 스위치 간에 취약한 프로토콜 인터페이스를 이용할 경우 전체 시스템을 공격에 대해 취약하게 만드는 요인이 될 수 있음.
- SDN/NFV 인터페이스 구성상 취약점을 악용하여 SDN 컨트롤러와 스위치 통신의 무결성과 기밀성에 대한 공격, 스위치와 컨트롤러 무단 제어 또는 자원 고갈 DoS 공격이 발생할 수 있음
- 예를 들어, SDN 컨트롤러를 공격하여 SDN 스위치의 플로우 테이블을 소진시키는 포화 공격이 발생될 수 있음.
- 또한, SDN 컨트롤러와 응용 프로그램 간의 신뢰관계, 즉 응용 프로그램의 변경 또는 인증과 네트워킹 기능에 대한 권한 부여 이슈가 중요함
- 응용 프로그램의 인증 및 권한 부여에 대한 강력한 메커니즘이 없다면 3rd Party의 악성 응용 프로그램이 SDN 컨트롤러로부터 네트워크 정보를 얻을 수 있음

*참조: 정보통신기획평가원(2019), '5G 네트워크 기술 진화에 따른 보안 이슈와 사이버대응 기술의 고려사항'

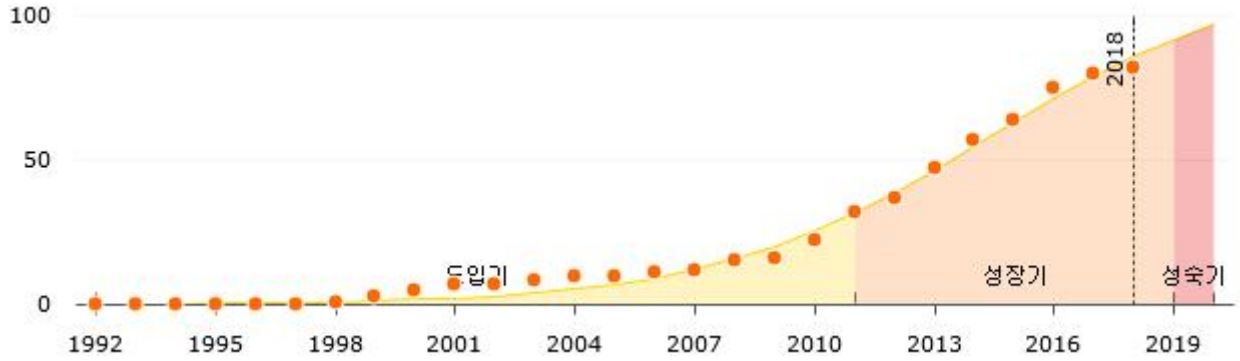
관련 기술의 미래 부상성

No.	Product family	K-Index	특허수	국내기업 점유율	기업 독점도	파급도	복합도	미래 부상성
1	SECURITY PROCESSOR	94.48	82	2.44%	562.17	1.45	0.84	3.95
2	★SECURITY CAMERA	94.27	473	10.57%	304.66	1.18	10.25	2.97
3	★NETWORK SECURITY SYSTEM	94.09	201	2.99%	343.59	0.08	4.34	3.16
4	SECURE ACCESSOR	93.11	41	2.44%	1,255.21	0.03	2.15	5.02
5	★SECURITY SYSTEM	92.38	3,448	1.42%	429.98	6.3	86.47	2.46
6	INTEGRATED SECURITY SYSTEM	91.38	32	0.00%	1,662.08	0	0.87	4.69
7	SECURITY MONITOR	90.79	84	2.38%	484.87	0.05	1.55	2.79
8	SECURITY SENSOR	90.54	70	0.00%	740.74	0.75	3.09	2.87
9	SECURITY CONTROLLER	90.48	84	4.76%	327.2	1.53	2.21	2.72
10	SECURITY MANAGEMENT SYSTEM	88.49	61	4.92%	314.94	0	1.22	2.51

*출처: 한국과학기술정보연구원(2019), TOD(Technology Opportunity Discovery)

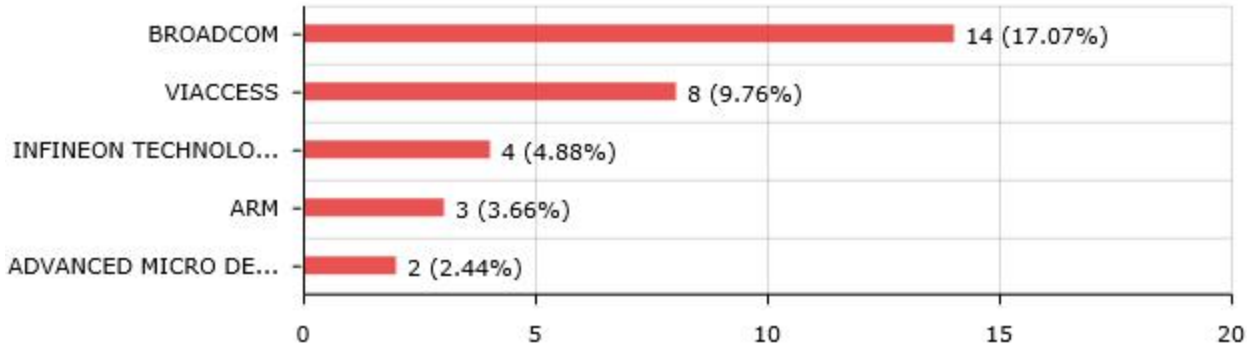
★는 KISTI 선정 TOP 2000 부상제품임

주요 Product family인 SECURITY PROCESSOR 분야의 특허수 성장성 예측



*출처: 한국과학기술정보연구원(2019), TOD

주요 Product family인 SECURITY PROCESSOR 분야의 주요 특허 출원인



*출처: 한국과학기술정보연구원(2019), TOD

문의처 DSU+

- ✓ 담당자 : 기술경영센터
- ✓ 전화번호 : 010-4312-3972
- ✓ 이메일 : sem903@dongseo.ac.kr
- ✓ 주소 : (47011) 부산시 사상구 주례로 47 동서대학교 산학력력단 기술경영센터