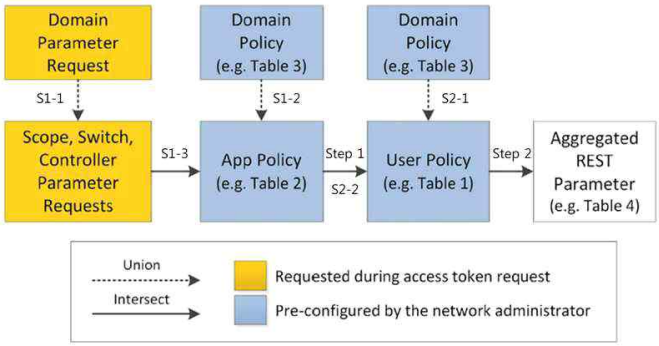
SDN에서 보안성 강화를 위한 REST 액세스 파라미터 충돌회피 방법

REST access parameter conflict avoidance method for security enhancement based on Software Defined Network



[대상 기술의 SDN에서 보안성 강화를 위한 REST 액세스 파라미터 충돌회피 방법의 블록구성도]

발명자 이상곤, 유스투스 에코 옥티엔, 임준휘

출원번호 10-2017-0092639
출원일자 2017-07-21
등록번호 10-1932505 (KR)
등록일자 2018-12-19

기술아젠다

- ✓ 안전한 사회 - 사이버 안전 및 정보보호
- ✓ 스마트한 사회 - 사공간 상의 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+

- 보안성 강화를 위한 RAPCA(REST Access Parameter Conflict Algorithm)을 제공함으로써, 기존에는 없는 구성을 통해 보안성을 강화하는 측면에서 효과를 극대화할 수 있는 효과를 제공
- 소프트웨어 정의 네트워크(Software Defined Network : SDN)에서 작동하는 스위치 장치(Switch)를 제어하는 제어기(Controller)에 대하여 사용자와 어플리케이션이 액세스 토큰(access token)을 요청할 때 사용하는 파라미터가 상호 상충되는 상황을 해결할 수 있는 효과를 제공

기술의 요지

- SDN에서 보안성 강화를 위한 REST 액세스 파라미터 충돌회피 방법에 관한 것으로, OAuthkeeper(1)가 액세스 토큰 요청을 검증하기 위한 절차를 적용하기 전에 REST 액세스 파라미터 요청을 도메인 파라미터 요청과 제 1 결합하고, 앱 정책과 도메인 정책과 제 2 결합을 수행한 이후, 제 1 결합과 제 2 결합 간의 공통되는 파라미터와 정책을 구하는 제 1 단계; 및 OAuthkeeper(1)가 상기 제 1 단계의 결과값에 해당하는 REST 액세스 파라미터와, 사용 정책 및 도메인 정책의 합집합의 결과에 대한 공통되는 파라미터와 정책을 구하는 제 2 단계; 를 포함함
- 이에 의해, 보안성 강화를 위한 RAPCA을 제공함으로써, 기존에는 없는 구성을 통해 보안성을 강화하는 측면에서 효과를 극대화할 수 있는 효과를 제공하고, 또한 소프트웨어 정의 네트워크(SDN)에서 작동하는 스위치 장치(Switch)를 제어하는 제어기에 대하여 사용자와 어플리케이션이 액세스 토큰을 요청할 때 사용하는 파라미터가 상호 상충되는 상황을 해결할 수 있는 효과를 제공

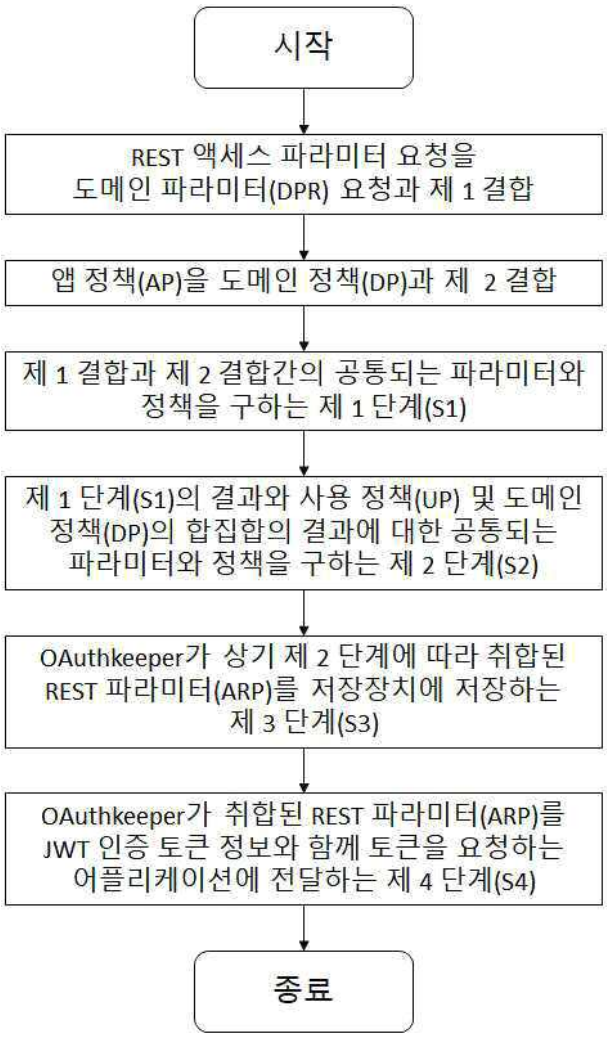
기존 기술의 문제점

- 네트워크 관리자는 네트워크 정책의 형식으로 전체 네트워크에 걸쳐서 사용자와 어플리케이션을 위한 REST 액세스 파라미터(REST access parameter)를 할당함. 더군다나, 어플리케이션은 OAuth2.0 액세스 토큰요청(access token request) 동안 추가적인 REST 액세스 파라미터(REST access parameter)를 요구
- 그래서 액세스 토큰 요청(access token request)으로부터의 REST 액세스 파라미터(REST access parameter)가 이미 존재하는 사용자/어플리케이션의 정책 파라미터들과 충돌함
- 또한, 사용자 또는 어플리케이션의 REST 액세스 파라미터(REST access parameter)가 다른 파라미터와 충돌할 수도 있음

개발 기술의 효과

- 보안성 강화를 위한 RAPCA(REST Access Parameter Conflict Algorithm)을 제공함으로써, 기존에는 없는 구성을 통해 보안성을 강화하는 측면에서 효과를 극대화할 수 있음
- 또한 소프트웨어 정의 네트워크(Software Defined Network : SDN)에서 작동하는 스위치 장치(Switch)를 제어하는 제어기(Controller)에 대하여 사용자와 어플리케이션이 액세스 토큰(access token)을 요청할 때 사용하는 파라미터가 상호 상충되는 상황을 해결할 수 있는 효과를 제공함

대표 도면



[SDN에서 보안성 강화를 위한 REST 액세스 파라미터 충돌회피 방법을 나타내는 흐름도]

기술의 작용

- 먼저, OAuthkeeper(1)가 액세스 토큰 요청(Access Token Request)을 검증하기 [0036] 위한 절차를 적용하기 전에 REST 액세스 파라미터 요청을 도메인 파라미터 요청(Domain Parameter Requests : DPR)과 제 1 결합하고, 앱 정책(App Policy : AP)과 도메인 정책(Domain Policy : DP)과 제 2 결합을 수행한 뒤, 제 1 결합과 제 2 결합 간의 교집합을 구한다(S1).
- 단계(S1) 이후, OAuthkeeper(1)는 단계(S1)의 결과에 해당하는 REST 액세스 파라미터(REST Access Parameter)와, 사용 정책(User Policy : UP) 및 도메인 정책(Domain Policy : DP)의 합집합의 결과에 대한 교집합을 구한다(S2).
- 단계(S2)를 완료하면, 주요 절차는 종료되어, 취합된 REST 파라미터(Aggregated Rest Parameter : ARP)이 생성된다.
- 이후, 결과적으로 OAuthkeeper(1)는 취합된 REST 파라미터(Aggregated Rest Parameter : ARP)를 저장장치에 저장된다(S3).
- 그리고 OAuthkeeper(1)는 취합된 REST 파라미터(Aggregated Rest Parameter : ARP)를 JWT(JSON Web Token) 인증 토큰 정보(JWT Bearer Token information)와 함께 토큰을 요청한 어플리케이션에게 전달한다(S4).

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

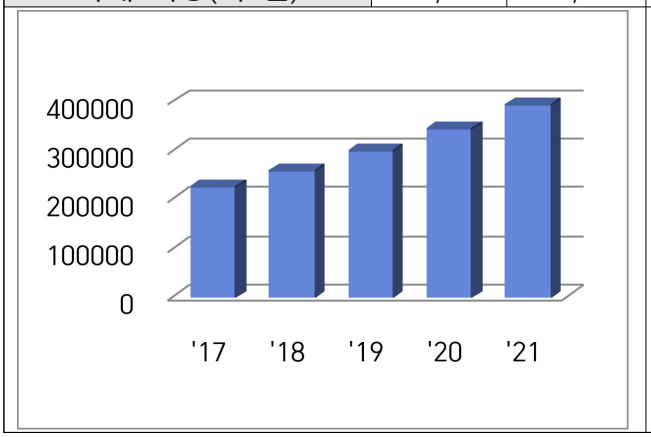
시장 규모

- 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

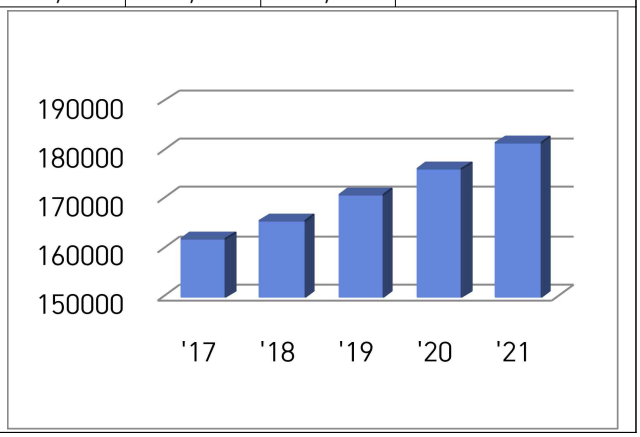
[표] 미국/국내 시스템 소프트웨어 개발 및 공급 분야의 시장규모 추이

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%



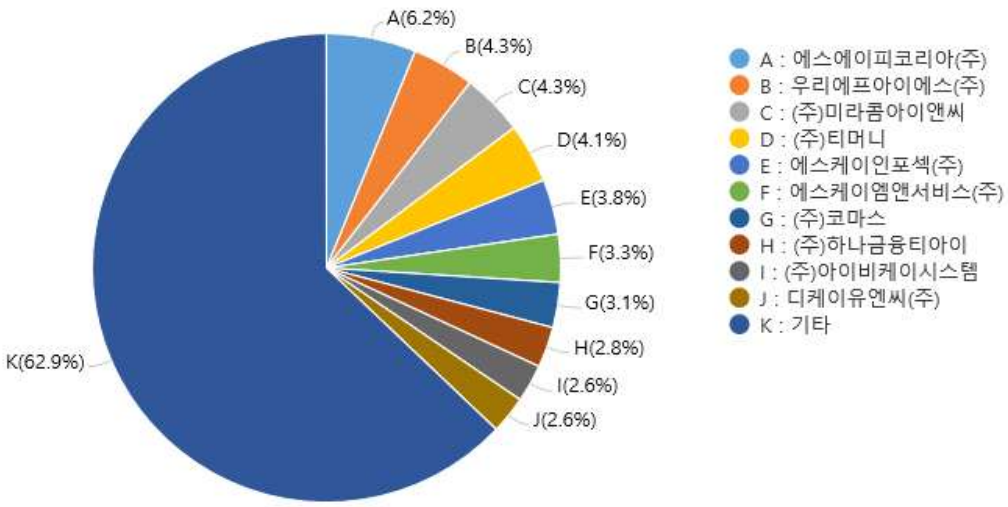
[미국 시장]



[국내 시장]

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

국내 시장 점유율



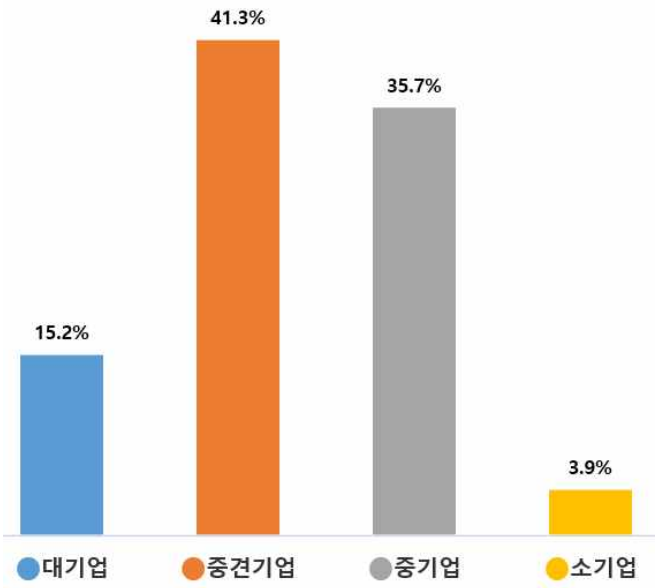
*출처: 한국과학기술정보연구원(2019, 2018년도 기준으로 작성)

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

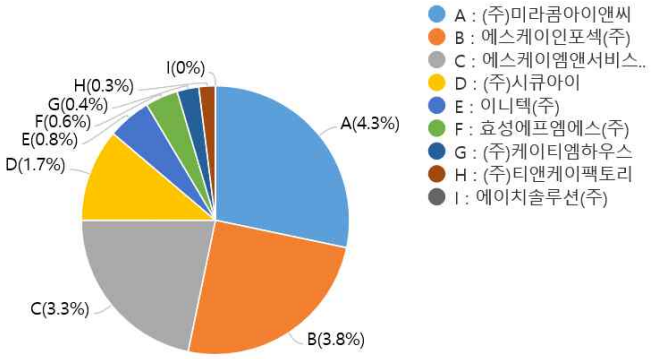
*출처: 한국과학기술정보연구원(2019)

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'

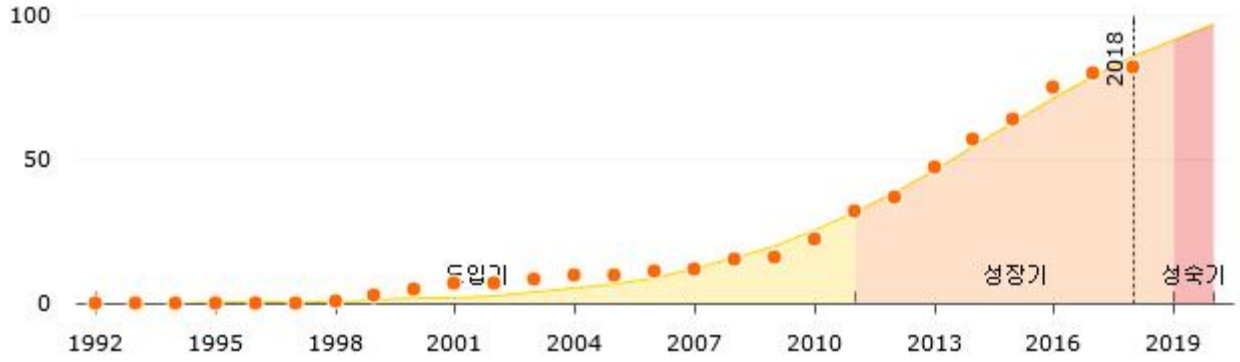
관련 기술의 미래 부상성

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)

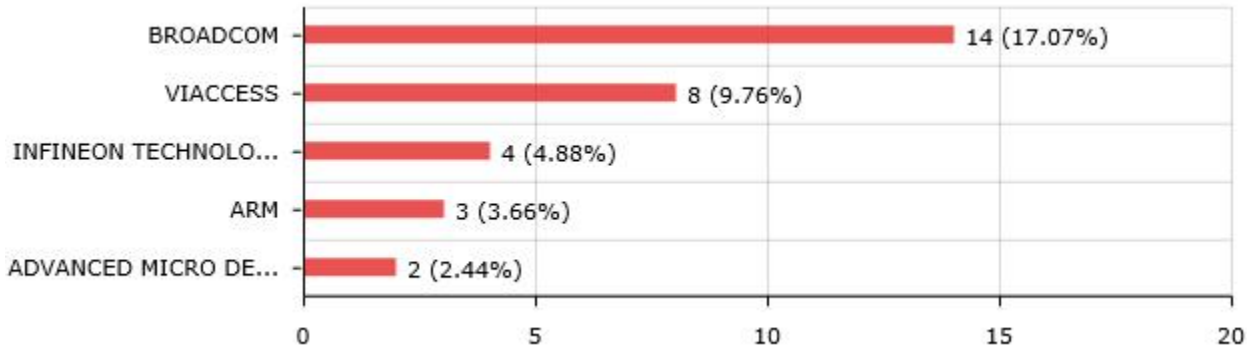
★는 KISTI 선정 TOP 2000 부상제품임

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