geni NETWORKS

SDN을 이용한 IoT환경 단말보안

2015.02

김계연

- 공개소프트웨어, 프리랜서 프로그래머
  - PC통신 에뮬레이터 신세대 개발
- 한글과컴퓨터, 두산정보통신
  - 한컴네트, 인터피아 ISP 운영 및 개발
- Yahoo! Korea
  - Chief Engineer, Yahoo Korea 서비스 런칭
- 어울림정보기술
  - 연구소장, SecureWorks Firewall / VPN 개발
- 지니네트웍스
  - 연구소장, Genian NAC / GPI 개발
- Technology
  - C/C++, Network, Security, Application Lifecycle Management

IoT 단말 환경변화

- 단말의 재정의
  - IT기능이 포함된 사내의 모든 자원
  - BYOD - 스마트폰, 태블릿 증가
  - IoT – 비 IT기기의 IT기기화, 다양한 Things에 대한 전문지식 필요
- Mobility 환경
  - 무선랜 필요성 증대
  - Static IP 시대의 종말
- 다양한 운영체제
  - Android, iOS, OSX, Tigen, WindowsPhone, BlackBerry…
- 지능화 고도화된 공격
  - IoT형 공격 – 비 IT기기를 통한 공격 (전기주전자, 전자담배), Denial of Power
  - 전력공급이 가능한 모든 자원에 대한 관리필요
  - East - West 공격 증가

소프트웨어 기반 단말보안의 한계

- 운영체제 종속
  - 윈도우즈 위주의 단말보안
  - 윈도우즈 점유율 하락
- 다양한 운영체제 지원의 어려움
  - 운영체제간 구현방식 보안수준의 차이
  - 모든 운영체제 지원 현실적 한계
- 사용자권한의 변화
  - 슈퍼유저 권한 미소유: Active Directory, iOS, Android
  - 전통적 보안기능 불필요: iOS의 App간 독립, KNOX - Sandbox
  - 보안기능 제공 제한적
- 새로운 IT 트랜드 지원의 어려움
  - 클라우드, 가상화, IoT

단말 보안의 새로운 흐름

- 단말에 대한 가시성
  - BYOD, IoT 단말에 대한 식별 - 사용자, 플랫폼, 타입, 연결방식

- 단말+네트워크 융합보안
  - 단말 소프트웨어 기반 분석 및 제어의 한계
  - 단말, 네트워크 독자적인 보안시스템에서 융합형 보안시스템으로 전환
  - 단말에서는 정보수집, 제어는 네트워크에서
  - 다양한 운영체제 지원에 적합

- 사람 및 프로세스 중심
  - 시스템 위주의 단말보안에서 사람중심, 프로세스중심의 보안으로 전환
  - 사용자 보안인식 향상이 가장 중요

제어 통제 방법의 변화

- 동적 단말 제어
  - 고정된 보안정책으로 통제불가
  - 식별기반, 관리자 인가, IT시스템 연계
- Multi-layer Enforcement
  - 에이전트: 사용자알람, 장치차단, 운영체제 설정
  - 네트워크: Filtering, Poisoning, Terminating
  - 인증: 802.1x, MAC Authentication Bypass
  - 연동: Firewall, UTM, VPN, 기타보안제품
- 기존 네트워크기반 제어의 한계
  - Inline Firewall, Connection Reset: 경계망 제어의 한계
  - Switch ACL: 동적제어의 어려움, Stateless
  - 802.1x, MAB, VLAN Steering: 서비스별 제어 불가
- SDN (Software Defined Networking)
  - End to End 접근제어에 가장 적합
  - OpenFlow, OpFlex, OnePK, VMWare NSX, OpenStack Neutron

동적 단말 제어

- 동적 네트워크 환경
  - DHCP 환경: MAC 기반 제어 필요
  - 사용자 기반 제어
- Device Fingerprinting
  - 단말 식별을 통한 제어 - 위험한 장치, 패치불가 장치, 알수없는 장치
  - 정확한 단말 식별이 중요, 로컬DB 필수
- 관리자 인가
  - 네트워크 접근 신청, 관리자 승인 프로세스 도입 필요
- IT 인프라 연계
  - 출입관리
  - 자산관리
  - API 필요

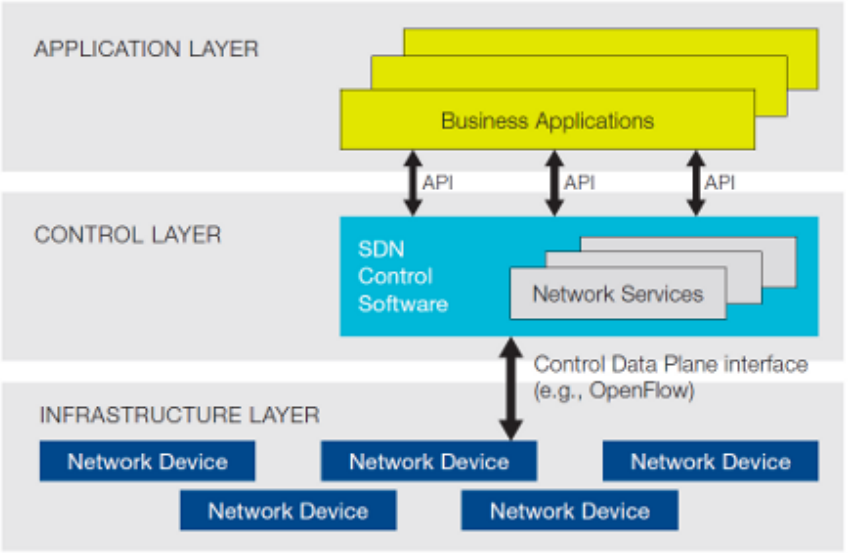
Software Defined Networking (SDN)

- 네트워킹에서 전송과 제어를 분리
  - Control Plain: 패킷의 흐름경로를 판단하는 Software
  - Data Plain: Control Plain에 의해서 결정된 흐름경로에 따라 패킷을 전달
  - 고성능 방화벽/L4 Switch에서 이미사용 (Fast Path / Slow Path)

- 네트워크 자동화
  - 네트워크 확장, 변경에 대한 자동대응

- 빠른 네트워크 대응
  - 새로운 서비스에 대한 대응력 강화
  - 사용자가 스스로 프로그래밍

- 비용절감
  - 어플리케이션 성능 확장과 데이터 플레인 성능확장을 분리
  - 밴더 종속성 탈피



단말보안과 SDN

- Access Control
  - 비인가 단말에 대한 차단 또는 서비스제한
  - End to End Firewall
  - MAC 주소 기반 접근제어 (Device 단위 접근제어)
  - 단말 플렛폼, 운영체제, 상태에 따른 제어정책 적용

- Network Tap
  - DPI가 필요한 특정한 단말, 서비스에 대한 패킷만 모니터링
  - L4 Switch / Smart TAP 역할 대체

- Limitations
  - FlowTable의 한계
  - 고가의 장비
  - Uni-directional Flow Table
  - Hierarchies of flows (FTP control / data)

SDN Deployment

- Pure SDN
  - 네트워크 기능 전체를 SDN화
  - 가상 네트워크, L2 Edge 네트워크

- Hybrid SDN
  - 일반 네트워크 기능은 기존대로 유지, ACL을 SDN으로 구현
  - 네트워크 안정성 유지, 장애시 빠른대처
  - Forward to Normal Action
  - Legacy Networking Stack 내장된 Hybrid SDN Switch 필요

- Distributed SDN Controller
  - WAN 구간이 많은 네트워크의 경우 Remote Controller Latency 문제
  - Remote 네트워크에 분산된 Controller 구축 필요
  - NAC Sensor를 Controller로 활용
  - OpenDaylight, ONOS등 개방형 Controller 탑재

SDN 기반 Endpoint 보안의 한계

- SDN on Edge Network
  - 아직은 고가의 SDN Switch. 저렴한 Whitebox Switch필요
  - 세션기반 제어를 위한 Flow Table 한계
  - WAN 환경을 위한 Low Latency SDN 콘트롤러 필요.
  - Branch Network에 존재하는 장비중 SDN 콘트롤러 기능제공 (NAC센서등)

- Stateless Slow
  - Statefull Filtering 미지원. FTP, H.323 등 계층적 Flow 처리불가
  - Session기반 감사기록 불가, Fragmentation 처리문제
  - 서비스기반 접근제어 한계
  - OpenFlow 1.5: Flow State 지원예정

- Deep Packet Inspection
  - 자체적인 DPI 미지원으로 Contents 기반 서비스 불가
  - L4 - L7 지원 예정. OpenFlow 1.5

Network Function Virtualization

- Virtual Appliance
  - 전용 Network Appliance 대체
  - Hardware 와 Software의 종속성을 제거
  - Software Defined Security시대 도래

- NFaaS (Network Function as a Service)
  - 임대형 네트워킹/보안 서비스
  - 가상화, 클라우드 환경 IT보안의 새로운 페러다임
  - ON.LAB ONOS (Open Network Operating System)

- Cloud Networking
  - Control Plane 을 Cloud 에서 서비스로 제공
  - Cisco Meraki, Aerohive등

Software Defined Security

- Security Apps
  - 개별적인 Security Enforcer가 필요가 없어지게 됨
  - Netwokring Platform위에 탑재되는 App
  - OpenFlow SDN, VMWare NSX, Cisco ACI, Network Operating System등
- Visibility
  - 위치적 제약이 없음. Local Device, Broadcast, M2M Visibility
- Distributed
  - Network Entry Point에서 직접적인 통제
  - 다수의 Enforcer를 통합하여 관리
- Orchestration
  - Intranet 전체를 관장하는 계층적 분산형 정책
  - 보안기능의 통합관리
  - 외부 시스템과의 연동을 통한 확장성이 중요

Genian NAC Suite

- Network Access Control
  - 국내 NAC 시장점유율 1위. 600여 고객 NAC 구축
- Intranet Security Platform
  - 통합 Endpoint / Network Security Platform
  - Network Access, 인증, IP관리, 패치관리, Desktop Security, 802.1x
  - Wireless Security, Device Control, NMS
- Distributed Enforcement
  - 내부망 접근제어를 위해 각 Network Segment마다 NAC Sensor를 설치
  - 접근 단말에 대한 정보수집 및 통제
  - 1,000대 이상의 Enforcer를 동시에 관리
- SDN Enforcer
  - NAC Sensor에 OpenFlow Controller 탑재
  - OpenFlow Switch에 Proactive Policy 적용을 통한 단말제어
  - Cisco ACI, VMWare NSX등 다양한 Enforcer 지원예정

감사합니다

지니네트웍스(주)