한국사물인터넷학회논문지 Vol. 2, No. 1, pp. 17-21, 2016 http://dx.doi.org/10.20465/KIOTS.2016.2.1.017

사물인터넷 서비스를 위한 소프트웨어 정의 네트워크 기술의 보안 분석을 위한 F(I)MEA 기법 적용

김그린[1], 한근희[2*], 김기천[3]
[1]건국대학교 IT융합 정보보호학과, [2]고려대학교 정보보호대학원, [3]건국대학교 컴퓨터공학과

An Adaptation of F(I)MEA Technique for security analysis on Software Defined Network Technology for IoT services

Green Kim[1], Keun-Hee Han[2*], Kee-Cheon Kim[3]
[1]Division of IT Convergence Information Security, Konkuk University
[2]Graduate School of Information Security, Korea University
[3]Division of Computer Science and Engineering, Konkuk University

요 약 사물인터넷의 급격한 발전은 기존에 존재하지 않던 형태의 새로운 서비스를 이끌어내었고, 이는 곧 기존 네트워크에 대한 변화를 요구하였다. 이러한 변화를 수용할 수 있는 기술 중 하나로 소프트웨어 정의 네트워크 기술을 이야기 할 수 있다. 소프트웨어 정의 네트워크 기술은 네트워크의 유연성 및 확장성을 제공한다는 점에서 큰 장점을 지니고 있지만, 이는 곧 보안의 취약점으로 악용될 가능성을 지니고 있다. 본 논문에서는 사물인터넷 서비스를 위한 소프트웨어 정의 네트워크 기술의 보안 분석을 위한 F(I)MEA 기법 적용에 대하여 다루고자 한다.

주제어 : 보안, 사물인터넷, 소프트웨어 정의 네트워크, F(I)MEA

Abstract The rapid development of IoT leads new kinds of services which does not existed. And, it requires several changes on existing network. Software Defined Network is one of the future network technology which can deal with problems from these kinds of changes. The strong point of Software Defined Network is flexibility and scalability. However, In some cases, these factors could be the security vulnerabilities. In this paper, we present adaptation of F(I)MEA technique for the security analysis on Software Defined Network Technology for IoT services.

Key Words : Security, IoT, Software Defined Network, F(I)MEA

1. 서론

사물인터넷 시장은 급격한 속도로 성장을 거듭해오고 있으며, 이에 따라 사물인터넷 발생 초기에는 지원하지 않았던 다양한 측면의 서비스에 이르기까지 그 영역을 점차 확대해가며 우리의 삶의 필수 불가결한 존재로 자리 잡고 있다. 이러한 동향에 힘입어 기존과는 다른 요구사항을 지닌 새로운 형태의 서비스들이 대거 등장하기 시작했으며, 이는 곧 사물인터넷 환경을 이루는 기반이 되는 네트워크 인프라에 대한 변화를 요구 하였다.

요구되는 변화 중 가장 큰 비중을 차지하는 부분은 기존 네트워크에 대한 유연성 및 확장성 증대에 대한 요구

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업(IITP-2016-H8501161012000l002) 및 글로벌 딜리버리 클라우드 플랫폼의 대규모 OTT 서비스 적용을 위한 방송·통신 사업자 공동의 시범 사업의 연구결과로 수행되었음(No.B0511-15-0001)."
*교신저자 : 한근희(khhan@formal.korea.ac.kr)
접수일 : 2016년 3월 15일, 수정완료 : 2016년 3월 20일, 최종게재확정 : 2016년 3월 30일

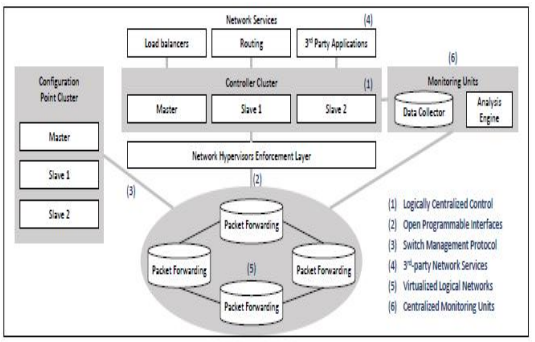
사항이라고 볼 수 있다. 이를 해결하기 위한 방안으로 곧 새로운 형태의 네트워크를 도출해 내기 위한 연구들이 이루어지기 시작했으며, 이를 수용할 수 있는 대표적인 미래 네트워크 기술 중 하나로 소프트웨어 정의 네트워크를 이야기 할 수 있다. 소프트웨어 정의 네트워크는 기존의 고정되어 유연하게 활용할 수 없었던 네트워크의 형태와는 달리 control plane과 data plane을 분리하여 기능적 측면에서의 사용 용이성을 도모하며 컨트롤에 대하여 프로그래밍이 가능하다는 측면에서 유연성 및 확장성에 대한 큰 장점을 지니고 있다.

소프트웨어 정의 네트워크는 이러한 장점을 토대로 빠른 속도로 발전을 거듭해오고 있지만, 이는 곧 치명적인 보안 위협으로 작용하기도 한다. 대표적인 예로, 중앙 집중식의 소프트웨어 정의 네트워크의 경우 네트워크 장비가 지니고 있는 flow table 한계를 표적으로 한 Denial-of-Service 공격의 표적이 될 수도 있으며, 소프트웨어 정의 네트워크의 아키텍처를 고려해볼 때, 아키텍처를 구성하는 각각의 요소들 사이에서도 취약점이 발생할 수 있는 측면에 대하여 생각해볼 수 있다. 그렇기에, 현재 구현 단계를 거쳐 실제 네트워크 시장에 도입되는 움직임을 보이고 있는 소프트웨어 정의 네트워크의 보안성을 확보하기 위한 보안 분석은 필수적 절차로 다루어져야 한다고 이야기할 수 있다.

본 논문에서는 사물인터넷 환경의 보안에 대하여 보장할 수 있는 방안을 찾기 위한 방안으로, 보안성이 향상된 소프트웨어 정의 네트워크 환경을 구축하기 위한 보안 분석 기법에 대해 다루고자 한다. 이를 위한 방안으로, F(I)MEA 방법을 적용하여 현 소프트웨어 정의 네트워크가 지닌 보안상의 문제점에 대해 인지하고 이를 개선하는 방향으로 나아갈 수 있는 방법을 모색하고자 한다.

2. 소프트웨어 정의 네트워크 보안

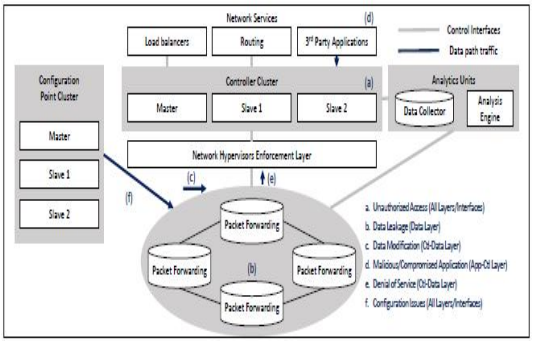
소프트웨어 정의 네트워크 또한 기존의 네트워크가 지니는 보안 요구 사항이 지니는 것과 마찬가지로 보안을 위해선 보안의 대상이 되는 요소를 식별하고, 보안 목표에 대하여 설정하는 것이 가장 우선적으로 수행되어야 한다고 볼 수 있다. 소프트웨어 정의 네트워크의 식별된 보안 요소의 경우 보안된 데이터, 네트워크 자산, 커뮤니케이션 트랜잭션 등을 이야기할 수 있으며, 보안의 목표의 경우 기밀성, 무결성, 가용성, 인증, 부인방지를 목표로 하고 있다. 보다 자세한 보안 사항에 대한 분석을 위하여 소프트웨어 정의 네트워크에 대한 특성을 살펴보면 Fig. 1과 같다.



[Fig. 1] Software Defined Network Characteristics

우선적으로는 네트워크의 가상화 및 추상적 view를 제공하는 논리적으로 중앙 집중 형태를 띠는 컨트롤 부를 이야기할 수 있다. 이는 곧 인터페이스에 대한 프로그래밍 가능성을 이끌어낼 수 있다. 또한 data plane을 이루는 하드웨어 기기들에 대한 설정과정을 수행하는 측면에서 switch 관리 프로토콜을 이야기할 수 있으며, 소프트웨어 정의 네트워크를 이용하는 어플리케이션에 대해서도 생각해볼 수 있다. 더불어, 소프트웨어 정의 네트워크의 지속적인 성능 향상을 위해 사용 되는 모니터링 부 또한 소프트웨어 정의 네트워크가 지니는 특성으로 볼 수 있다.

Fig. 1을 통해 살펴본 소프트웨어 정의 네트워크 특징을 대상으로 공격이 이루어질 수 있는 상황에 대한 도식화 즉 공격이 이루어질 수 있는 대상 및 취약점은 Fig. 2에서 설명하는 것과 같다.



[Fig. 2] Attacks and Vulnerabilities

control plane 측면에서는 비 인가된 사용자의 접근에 대해 이야기할 수 있다. 이는 컨트롤러에 대한 관리자 이외의 악의적인 의도를 가지고 접근하는 사용자를 의미한다. 또한 data plane 측면에서의 데이터 누수 현상에 대해서도 생각해볼 수 있다. 합법적이지 않은 경로를 통하여 악의를 가진 사용자가 접근하여 data plane에 대한 통제를 수행할 경우 하드웨어 장비 단에서 데이터에 대한 유출이 발생할 가능성을 지닐 수 있다. 데이터 누수와 더불어 생각할 수 있는 부분은 컨트롤 정보에 대한 수정이 이루어질 수 있다는 점이다. 소프트웨어 정의 네트워크의 핵심이라고 할 수 있는 control plane의 경우, data plane에 직접적인 명령을 내리게 되는데 악의적인 접근을 통해 이 명령에 대한 수정 절차가 발생할 수도 있다. 이외에도 어플리케이션 자체가 공격 양상을 띠는 경우 및 컨트롤러의 과부하를 일으켜 발생하는 Denial-of-Service 공격, 하드웨어를 직접적으로 공격하는 설정 부와 관련한 공격 및 이에 대한 취약점이 존재할 수 있다.

Fig. 2 에 대하여 보안위협이 될 수 있는 요소 및 공격 대상에 대한 분류는 Table 1과 같다.

[Table 1] Categorization of Security Issues

Security Issue/Attack	SDN Layer Affected or Targeted				
	Application Layer	App/Interface	Control Layer	CP/Data Interface	Data Layer
Unauthorized Access e.g. • Unauthorized Controller Access/Controller Hijacking • Unauthorized/Unauthenticated Application	X	X	X X	X	X
Data Leakage e.g. • Flow Rule Discovery (Side Channel Attack on Input Buffer) • Credential Management (Keys, Certificates for each Logical Network) • Forwarding Policy Discovery (Packet Processing Timing Analysis)			X	X	X X X
Data Modification e.g. • Flow Rule Modification to Modify Packets (Man-in-the-middle attack)			X	X	X
Malicious/compromised Applications e.g. • Fraudulent Rule Insertion	X	X	X		
Denial of Services e.g. • Controller-Switch Communication Flood • Switch Flow Table Flooding			X	X	X X
Configuration Issues e.g. • Lack of TLS(or other Authentication Technique) Adoption • Policy Enforcement • Lack of Secure Provisioning	X X X	X X X	X X X	X X	X X
System Level SDN Security e.g. • Lack of Visibility of Network State			X	X	X

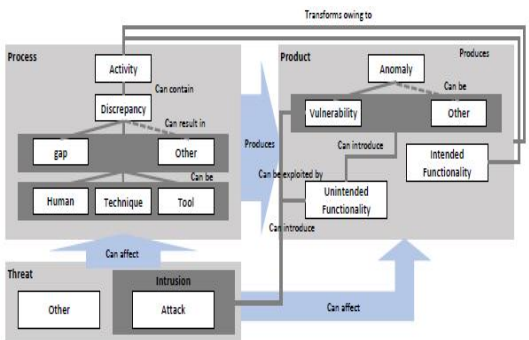
Table 1 은 앞서 제시한 보안 공격 및 취약점에 대한 분류를 기반으로 실제로 발생할 수 있는 보안 이슈 및 구체적인 공격을 바탕으로 분류되어 있으며, 각 보안 이슈 및 공격이 대상으로 하는 소프트웨어 정의 네트워크의 구성요소를 나타낸다. 이를 통하여 공격이 가장 많이 발생하는 구성 요소는 control plane과 data plane 측면임을 알 수 있으며, 보안을 고려할 경우 이에 대한 보안 분석이 보다 심도 있게 수행되어야 함을 알 수 있다.

3. F(I)MEA Technique

F(I)MEA Technique은 Failure (Intrusion) Modes and Effect Analysis를 의미한다.

3.1 Taxonomy of issues

F(I)MEA Technique을 이루는 기본이 되는 접근 방식은 process-product 접근 방식이다. 이는 가능한 문제에 대하여 결정하면 문제에 대한 구현을 통하여 결과를 얻을 수 있음을 의미하며, 예상한 결과와 실제 구현 결과의 차이인 'gap' 개념을 기반으로 한다. Fig. 3은 process-product 접근 방식을 도식화 하여 보여준다.



[Fig. 3] Process-Product approach

3.2 Analysis Technique

앞서 설명한 'gap' 개념은 정형화된 형태로 표현된다. 이를 표현하기 위한 가장 편리한 방법 중 하나로 기존 FMECA 기술을 변형하여 Intrusion Modes and Effects Criticality Analysis라 불리는 IMECA 기법이다.

식별된 각각의 gap은 하나의 IMECA 표로 나타나게 되며, gap을 표현하는 방식인 예상한 결과와 현재 시스템의 차이는 각 IMECA 표에 행으로 제시된다.

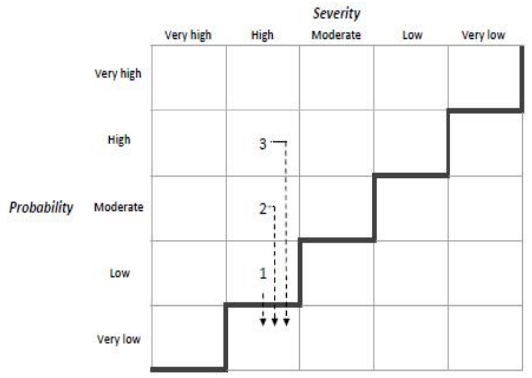
4. Case study of F(I)MEA Technique

이 장에서는 3장에서 설명한 F(I)MEA 기법을 소프트웨어 정의 네트워크에 적용한 case study에 대하여 다룬다. 2장에서 설명한 소프트웨어 정의 네트워크의 분류 중 Controller hijacking, Man-in-the-middle, Denial of Service를 대상으로 F(I)MEA Technique을 이용하여 분석을 수행한 예는 다음 Table 2와 같다.

[Table 2] Case Study

GAP No	Attack mode	Attack nature	Attack cause	Occurrence Probability	Effect Severity	Type of effects				
						Application Layer	App-CI Interface	Control Layer	CI-Data Interface	Data Layer
1	Controller hijacking	Active	• Weak authentication	Low	High	-	-	• Gain access to network resource • Manipulate the network operation		
2	Main-in-the middle	Active	• Weak Authentication • Weak confidentiality	Moderate	High	-	-	• Have control over the entire system • Insert/Modify flow rules in the network devices • Allow packets to be steered through the network to the attacker's advantage		
3	Denial of Service	Active	• Weak protection • Resource limitation of flow table	High	High	-	-	• Lead to fraudulent rule insertion and rule modification		

Table 2의 결과를 토대로 보안 분석 결과에 대하여 현재 보안 단계가 어느 단계에 위치해 있는지와 개선 방향에 대하여 확인하기 위해 ISO 31000 문서의 Criticality matrix를 통해 표현할 수 있으며 이에 대한 결과는 Fig. 4와 같다.



[Fig. 4] Criticality Matrix

5. 결론

본 논문에서는 사물인터넷의 발전이 요구하는 새로운 형태의 네트워크의 요구에 따라 등장한 소프트웨어 정의 네트워크의 보안 분석을 위하여 F(I)MECA 적용하는 연구를 수행하였다.

현재 네트워크의 기본적인 보안에 대한 요구 사항을 충족할 수 있는 보안에 측면의 강점을 지니고 있는 소프트웨어 정의 네트워크는 존재하지 않는다고 이야기할 수 있다. 이를 해결하기 위한 방안으로 지속적인 보안 분석을 바탕으로 소프트웨어 정의 네트워크가 지니는 공격에 대한 취약점에 대하여 식별하는 과정이 필수 불가결할 것으로 보여 진다.

REFERENCES

[1] AlgirdasAvizienis,Jean-ClaudeLaprie,BrianRandell,CarlLandwehr."BasicConceptsandTaxonomyofDependableandSecureComputing".Jan2004.

[2] M.Coughlin."ASurveyofSDNSecurityResearch".

[3] S.Scott-Hayward,S.Natarajan,S.Sezer"ASurveyofSecurityinSoftwareDefinedNetworks".CommunicationsSurveys&Tutorials,IEEE,2015.

[4] S.Scott-Hayward,G.O'CallaghanandS.Sezer"SDNsecurity:Asurvey",FutureNetworksandServices,IEEE,2013.

[5] R.Kloeti,"OpenFlow:ASecurityAnalysis,"Available:ftp://yosemite.ee.ethz.ch/pub/students/2012-HS/MA-2012-20-signed.pdf,2013.

[6] KevinBenton,L.JeanCamp,ChrisSmall."OpenFlowvulnerabilityassessment",ProceedingsofthesecondACMSIGCOMMworkshoponHottopicssoftwaredefinednetworking.2013.

[7] DiegoKreutz,FernandoM.V.Ramos,PauloVerssimo,"Towardssecureanddependablesoftware-definednetworks",ProceedingsofthesecondACMSIGCOMMworkshoponHottopicsinsoftwaredefinednetworking.2013.

[8] A.Gorbenko,V.Kharchenko,O.Tarasyuk,A.Furmanov"F(I)MEA-techniqueofWebServicesAnalysisandDependabilityEnsuring",LectureNotesinComputerScience,2006.

[9] E.Babeshko,V.Kharchenko,A.Gorbenko,"ApplyingF(I)MEA-techniqueforSCADA-basedIndustrialControlSystemsDependabilityAssessmentandEnsuring",DepCoS-RELCOMEX,2008.

[10] O.Illiashenko,V.Kharchenko,A.Kovalenko,"CyberSecurityLifecycleandAssessmentTechniqueforFPGA-basedI&Csystems",Design&TestSymposium,2013.

[11] ISO/IEC27000,Informationtechnology-Securitytechniques-Informationsecuritymanagementsystems-Overviewandvocabulary,InternationalOrganizationforStandardizationandInternationalElectrotechnicalCommission,2009.

[12] ISO/IEC27001:2005,Informationtechnology-Securitytechniques-Informationsecuritymanagementsystems-Requirements,InternationalOrganizationforStandardizationandInternationalElectrotechnicalCommission,2005.

[13] ISO/IEC27002:2005,Informationtechnology-Securitytechniques-Codeofpracticeforinformationsecuritymanagement,InternationalOrganizationforStandardizationandInternationalElectrotechnicalCommission,2005

[14] ISO31000,RiskManagement,Riskassessmenttechniques,InternationalOrganizationforStandardizationandInternationalElectrotechnicalCommission,2009.

김 그 린(Green Kim)

- 2015년 2월 : 건국대학교 컴퓨터공학부 (학사)
- 2015년 2월 ~ 현재 : 건국대학교 일반대학원 IT융합정보보호학과 석사과정

<관심분야>
사물인터넷 보안, 네트워크 보안, 미래인터넷 보안

한 근 희(Keun-Hee Han) [정회원]

- 서울과학기술대학교 컴퓨터공학과 졸업
- 한양대학교 공학대학원 공학석사
- 고려대학교 대학원 이학박사
- 현재 : 고려대학교 융합소프트웨어전문대학원 산학교수

<관심분야>
소프트웨어 보증, 시큐어 코딩, 정보보호관리 체계, 개인정보보호, 클라우드 컴퓨팅 보안, 스마트 의료 보안, 스마트 공장 보안 등

김 기 천(Kee-Cheon Kim)

- 1988년 : 서울대학교 계산통계학 (공학사)
- 1992년 : 미국 Northwestern Univ. (공학박사)
- 1992년 ~ 1996년 : 한국통신기술(주) 선임연구원
- 1996년 ~ 1998년 : 신세기 통신(주) 책임연구원
- 1998년 ~ 현재 : 건국대학교 컴퓨터공학과 교수

<관심분야>
mobile wireless network, 미래인터넷 보안, sensor network, 네트워크 보안, 사물인터넷