미래 인터넷 보안 연구 동향 분석 : FIA를 중심으로★

전은아* · 이도건* · 이상우** · 서동일** · 김점구***

요 약

미래인터넷은 현 인터넷 구조의 한계를 극복하여 미래의 새로운 요구사항을 수용하기 위해 Clean-slate에 기반을 둔 설계와 개발이 국내·외에서 활발히 이행되고 있다. 미래인터넷 관련 연구개발은 이미 미국, 유럽 등의 선진국에서 정부의 대규모 투자와 지원이 이루어져 미래인터넷 연구 프로그램이 추진되어 진행되고 있다. 미래인터넷의 세부 기술의 특성을 기준으로 인프라 기술, 아키텍처, 그리고 서비스 기술 분야로 구분된다. 우리나라는 특히, 인프라기술과 서비스 기술은 우위에 있는 분야이다. 이러한 기반 서비스를 미래 인터넷에 접목하기 위한 신뢰통신에 대한 연구 및 기술 개발은 경쟁력을 가질 수 있는 분야이다. 이에 본 논문에서는 미래인터넷을 위한 신뢰통신 참조모델 검증 기술 연구를 위해 미국 NSF 4개 과제에서 보안 기술 분석과 각 구조에서 보안 기능 분석에 대하여 설명한다.

Study on Trends of the Future Internet Security : FIA Work

Jun Eun-A* · Lee Do-geon* · Lee Sang-Woo** · Seo Dong il** · Kim Jeom Goo***

ABSTRACT

Future Internet has been designing and developing in the world because of overcoming limits of current Internet and accepting new requirements. Therefore it is totally different from architectures of current Internet and it is based on Clean-Slate. Future Internet already has been studying with enormous investment by advanced countries such as USA, EU etc. Technical characteristics of Future Internet can be categorized into Infra techniques, Architectures and Service techniques. Especially, our country is in a superior position in Infra techniques and Service techniques. We can have competitiveness to develop trust communication in Future Internet because we have advantages of various Services such as mobile communication, Machine to Machine and Sensor Networks. This paper aims to analysis reference model of trust communication in Future Internet. To achieve this, we studied analysis of security techniques in four Future Internet researches of NSF.

Key words : Future Internet, FIA(Future Internet Architecture), NDN, MobilityFirst, Nebula, XIA, FI Security

접수일(2012년 2월 23일), 수정일(1차: 2012년 3월 13일), 게재확정일(2012년 3월 19일)

★ 본 연구사업은 지식경제부의 출연금 등으로 수행하고 있는 한국전자통신연구원의 정보통신연구개발사업 위탁연구과제 연구결과입니다.

* 고려대학교 정보보호대학원
** ETRI(한국전자통신연구원)
*** 남서울대학교 컴퓨터학과

1. 서 론

현재까지 인터넷은 많은 변화를 거쳐 오늘날의 모습을 이루게 되었지만, 통신환경의 급격한 변화와 다양한 사용자의 요구사항의 증대로 인해 현재의 인터넷이 갖는 근본적인 수많은 문제점들이 발견되어 왔고, 이러한 문제점을 수정하기 위하여 많은 기술들이 연구개발 되어 오늘날의 거대한 인터넷이 구성되어져 왔다. 그러나 미래인터넷에서는 다른 형태의 서비스들과 요구사항들이 필요할 것으로 예상되고 있으며, 이에 대하여 현재 인터넷이 가지는 기본적인 구조를 수정하지 않고 새로운 기능과 보완점들을 수용하는 방법의 대처는 한계를 가질 수밖에 없다. 현재 인터넷의 구조 자체가 가지는 문제점 중 서비스 방식 및 기술, 보안 등에 대한 취약점들에 대하여 효율적인 수정 하는 것은 불가능하기 때문에 미래인터넷은 clean-slate의 개념으로 설계 및 개발될 새로운 인터넷에 대한 연구가 활발히 진행되고 있다.

미래인터넷 연구에서 개선하고자 하는 네트워크 기술 사항은 다음과 같다. 라우팅 확장성(Routing Scalability), 보안성 및 견고성(Security and Robustness), 이동성(mobility), 자율성 및 관리성(Autonomous and Manageability), 서비스 품질(Quality of Service), 이질성(Heterogeneity), 주문성, 프로그램화 및 재설정(Customizability, Programmability and Re-configurability), 데이터 중심 및 상황인지(Data-centric and Contex-awareness), 경제적 동기(Economic incentives) 등이다.

미래인터넷에 대한 설계 요구사항에서 반영하듯이 미래인터넷 정보보호 요구사항은 무엇보다, 사용자들에게 적절하며, 수준별로 정보보호 기능을 지원하기 위해 매우 다양한 형태로 구현되어질 필요가 있다.

그러나 이러한 문제는 정보보호와 서비스 제공의 입장에 따라 정보보호의 기능 및 강도가 달라진다. 이러한 문제점을 인식하여 ITU-T 미래 네트워크에서 고려해야 할 정보보호 요구사항에 대하여 규정한 바가 있으며, X.805 권고안 [ITU-X.805]에서 종단간 네트워크 정보보호를 위한 권고를 하고 있다. 권고안에서는 사용자의 종단간 종신 접속을 위협할 수 있는 여러 가지 요인들에 대한 요구사항으로 접근제어(Access control), 인증(Authentication), 부인봉쇄(Non-Repudiation), 데이터 기밀성(Data confidentiality), 통신보안(Communication security), 데이터 무결성(Data integrity), 가용성(Availability), 프라이버시(Privacy) 등의 정보보호 기능을 제공해야 한다고 명시하고 있다 [1].

또한, ITU-T Y.2701 [24] 권고안에서는 이러한 8가지 정보보호 기능에 대해서 차세대네트워크(NGN, Next Generation Network)에서 제공하여야 할 기능으로 Access Control, Authentication, Data Confidentiality, Non-reputation, Communication Security, Data integrity, Availability, Privacy 등을 권고하고 있다.

그러나 미래인터넷 정보보호 기능에 대해서 명확한 요구사항과 해결책은 제시되지 못하고 있는 상황이며, 연구의 경우 초기단계에 머무르고 있는 실정이다.

이에 본 논문에서는 미래인터넷의 국내・외 연구동향에 대하여 살펴보고, 특히 미래인터넷 보안성을 해결하고자 미래인터넷 보안 기술의 동향을 FIA 연구에서의 보안기술에 대한 분석에 대하여 설명한다.

2. 미래인터넷 국내・외 연구 동향

미래인터넷은 현재 통신환경의 급격한 변화와 다양한 요구사항의 증대와 새로운 구조의 네트워크와 프로토콜이 필요하다는 문제의식에서 기인하여 미국, 유럽, 일본 등의 주요 선진국은 현재 인터넷의 한계를 해결하고 전송품질의 보장, 이동성, 완벽한 보안 및 새로운 융합서비스를 확장, 수용할 수 있는 개념의 미래인터넷에 대한 연구 개발 프로그램을 정부의 주도로 추진중에 있다.

미국, 유럽 등의 주요 선진국은 2005년부터 미래인터넷에 대한 기술 개발 및 산업화 주도권 확보를 위해서 정부전담의 추진 조직을 신설하고 대규모 투자를 시행하여 테스트 인프라를 중심으로 연구・개발・시험을 동시에 추진하는 모델 및 산업계가 적극 참여하여 연구결과를 상용화하기 위한 작업을 활발히 진행중에 있다.

2.1 미국

미국은 기존의 인터넷을 주도해왔으며, 일찍이 현재 인터넷 구조가 가지는 한계 및 문제점 대응방안에 대한 네트워크의 필요성 및 방향성을 인식하고 연구를 시작해 오고 있다. 2000년 초기부터 수행된 DARPA (Defence Advanced Research Projects Agency)의 NewArch 프로젝트에서 처음으로 인터넷을 현재, 미래의 요구사항을 기반으로 다시 설계에 대한 시도를 했다[28]. 2003년 NSF[26]의 Clean-slate 프로젝트 및 SIGCOMM FDNA workshop 등에서의 논의를 통해 본격적인 미래인터넷 연구의 필요성을 인식하고, NSF는 미래인터넷 연구를 위해 FIND [17] 프로그램과 미래인터넷 테스트베드 개발을 위한 GENI 프로젝트 [21, 22]를 시작하였다.

GENI 프로젝트의 주도 업체인 GPO(GENI Project Office)는 관련기술 R&D 업체인 BBN Technologies가 선정되었으며, BBN은 미국 14개 대학 캠퍼스 및 리서치 백본 네트워크 2개에 GENI 플랫폼을 구축하는 작업을 하였으며, 2009년 GENI Control Framework Cluster의 구축을 위하여 GENI control framework의 실행을 위한 프로젝트들을 5개 Cluser로 통합하였으며, GENI Spiral 1의 마일스톤(milestone)을 분석, 계획, 설정하였으며, GENI Engineering conference에서 Cluster 별로 프로젝트를 시연하였다. GENI 프로젝트의 인프라 구축은 세 가지 형태의 대규모 실험용 네트워크 인프라를 구축하는 것으로, 그 특징은 Programmability, 가상화 및 자원 공유, federations, Slice 중심의 실험을 들 수 있다.

2.2 유럽

유럽의 미래인터넷 연구는 EU를 중심으로 기술·사회·경제 등 종합적 측면의 3대 연구영역과 6대 세부 연구 분야로 나누어 진행하고 있으며, 신뢰기반 네트워크 및 서비스인프라 구축 계획 (Pervasive and Trusted Network and Service Infrastructure)을 기본으로 하는 미래인터넷 연구는 향후 15년 후 도래할 미래 네트워크와 서비스에 유럽이 유연하게 대응하고 핵심 역할을 수행할 수 있는 미래인터넷 개발을 위한 실험적 R&D(experimentally-driven approach) 추진하고 있다.

2007년부터 총 7년의 사업기간을 잡고 FP7(7thFrameworkProgramme)ICTChallenge1,FIPPP(FutureInternetPublicPrivatePartnership)등 미래인터넷 R&D 및 민관협력을 추진하고 있으며, 6개의 기술 영역 그룹으로 나누어 세부 연구 과제를 진행 중에 있다. 그 내용은 다음과 같다.

- 미래 네트워크(The Network of the Future)
- 서비스, S/W, 가상화 측면 인터넷(Internet of Services, Software and Virtualization)
- 사물 인터넷(Internet of Things and Enterprise environments)
- 신뢰 IT기술(Trustworthy ICT)
- 네트워크 미디어와 3D 인터넷(Networked Media and 3D Internet)
- FIRE(sub project)

특히, 신뢰 정보통신 기술을 위하여 신뢰기반 네트워크/서비스 인프라 기술과 툴, 표준화, 인증 모델에 대한 연구를 진행하고 있다. 2009년부터 진행하고 있는 ICT(Information and Communication Technology)의 신뢰성 제고(Trustworthy ICT)를 위한 목표성과는 네트워크 인프라의 신뢰성제고, 서비스 인프라의 신뢰성 제고, ICT의 신뢰성 제고를 위한 기술 및 툴의 개발을 주 연구 분야로 진행하고 있다. 또한 미래인터넷의 기술적인 측면 이외에도 연구개발 과정에 산업과 이용자(end-users)의 참여를 통해 비즈니스 및 규제정책 안건에 관한 연구도 병행하는 연구 추진 방향을 기획, 운영하고 있다.

2.3 한국

국내의 미래인터넷을 위한 미국과 유럽의 선진국과 같은 국가 차원의 전략적인 추진 체계나 중장기적인 계획 수립과 예산지원은 아직은 초기 단계이다. 2006년 9월 국내외의 활발한 미래인터넷 교류를 위하여 학계와 연구소를 중심으로 “미래인터넷 포럼”을 처음 설립하여 아키텍처 WorkGroup, 무선 WG, 서비스 WG, 정책 WG, 테스트베드 WG의 분야로 연구를 시작하였다. 현재 국가 차원의 전략을 세우고 시작하는 단계의 국내 미래인터넷 연구에 대한 비전은 새로운 패러다임

인 미래인터넷 원천기술의 확보와 글로벌 시장을 선점하여 향후 인터넷 경제의 국가 경쟁력을 확보하는 비전을 설립하였다. 이를 위한 전략으로 미래인터넷 IT 인프라 분야의 국가적 사안으로 설정하고, 산업과 연계한 연구개발 전략 등 중장기 기본계획을 수립하여 추진하고 있다. 국내에서도 2006년 9월 미래인터넷 포럼 등을 발족하여 학계를 중심으로 다양한 미래인터넷 아키텍처 기술연구를 진행하고 있다. 미래인터넷의 아키텍처, 무선기술, 서비스, 테스트베드, 정책 등의 5개의 워킹그룹을 구성하고 미래인터넷에 대한 논의를 시작하였다. 특히, 2009년부터 ETRI및 KITSI는 미국 GENI 프로젝트와 연계하여 미래인터넷 테스트베드 구축을 위한 “미래인터넷을 위한 가상화 지원 프로그래머블 플랫폼 기술”이라는 제목 하에 테스트베드용 가상화 플랫폼 개발 진행 중에 있다.

2010년부터 KISA에서 미래인터넷 정책 추진 체계 정립 및 중장기 기본계획 수립 등 국가 차원의 미래인터넷 지원・육성사업이 활발히 추진 중에 있다. 최근 ETRI와 미래인터넷포럼을 중심으로 미래인터넷에 대한 연구가 많이 진행되고 있다. 그러나 무엇보다 선행되어야 하는 신뢰통신 구조에 대한 고려와 연구는 아주 미진하게 진행되고 있는 실정이다.

3. 미래 인터넷 보안 기술 분석 (NSF 의 FIA 프로젝트를 중심으로)

FIA(Future Internet Architecture) 프로젝트는 미래인터넷 아키텍처 요구사항을 도출하고 이를 기반으로 아키텍처 프로토타입 구현 및 테스트를 위해 가장 기본적으로 고려되는 요구사항으로 보안(Security), 사생활 보호(Privacy), 신뢰성(Reliability), 이용성(Usability) 등과 관련된 아키텍처 신뢰도(Trustworthiness) 이며, 이 밖에도 조정성(scalability), 개방성(openness), 유비쿼터스 액세스(Ubiquitous access), 혁신성(Innovation-enabling), 관리성(manageability), 진화성(Evolvability), 경제적 실효성(economic viability) 등이 주된 고려사항이다. NSF에서 추진 중인 FIA는 2010년 8월경에 시작하였으며, 연구내용별로 다음 4개의 세부 연구 프로젝트로 구성되어 있다.

- NDN: UCLA 외 9개 기관 연구. 콘텐츠 중심 FI (Future Internet)
- MobilityFirst: Rutgers University 외 7개 기관 연구. 이동성 중심의 FI
- NEBULA: University of Pennsylvania 외 11개 기관 연구. 클라우드 중심의 FI
- XIA: Carnegie Mellon University 외 2개 기관 연구. 보안성 중심의 FI

본 장에서는 FIA 4개 프로젝트인 NDN, MobilityFirst, Nebula, XIA의 기술, 구조 및 보안 기능 대하여 분석한다.

3.1 NDN 보안기술 분석

NDN(Named Data Networking)은 기존 인터넷의 전통적인 통신방식인 클라이언트 서버 모델(Client-server model)을 기반으로 하고 있으며, 이러한 모델에서 통신에 참여하는 이해관계자들이 협력관계를 구축한 후, IP 데이터 패킷을 단일한 경로를 통해 전송하는 방식을 채택하고 있다. 그러나 현재 다양한 콘텐츠의 생성 및 전송 등에 초점을 맞춘 통신방식이 주로 사용되고 있지만, 기본적인 클라이언트 서버 모델은 미래에 제공 될 다양한 서비스와 애플리케이션에 대한 콘텐츠 보안기능을 지원하는 메커니즘은 현재 구축되어 있지 않는 현실이다.

이에, NDN 프로젝트는 address, server, host 등의 위치 “Where”(호스트 또는 서버의 주소) 중심이 아닌, 무엇 “What” (사용자가 원하는 콘텐츠) 중심으로 네트워크 구조 변화를 취하고 있다. 즉, 사용자가 특정 콘텐츠를 요청할 때, 해당 콘텐츠 서버에서 특정 콘텐츠를 제공하는 것이 아니라, 네트워크상에서 해당 콘텐츠를 캐싱하고 있는 네트워크 노드가 사용자에 콘텐츠를 제공하는 방식으로 네트워크를 설계하고 있다. 즉, IP어드레스와 같은 위치를 지정하는 대신, 데이터 네이밍(naming)을 수행하여 데이터를 최상의 독립적 주체(first-class entity) 로 진화시키는 것이다.

NDN의 보안기능은 서명의 효율성(Efficiency of Signatures), 신뢰관리의 사용, (Usable Trust Management), 네트워크 보안과 대응(Network security and Defence)를 제공한다. 각각 제공하는 보안 기능 분석은 다음과 같다 [25].

- 콘텐츠 기반 보안

- NDN은 Names와 콘텐츠를 포함하여 모든 콘텐츠 인증을 수행
- Data Packet의 “Signed Info” 에 서명에 관련된 정보
- Cryptographic digest, 공개키의 fingerprint, public key, identifier 등
- Private Content는 필요 시 암호화되어 전송될 수 있음

• End-to-End 보안과 프라이버시
- Publisher와 Content consumer 사이의 End-to End 보안 제공
- 중간 노드(라우터)에서는 콘텐츠 제공자와 사용자의 위치와 정보를 알 수 없음
- 모든 Data Packet의 names와 콘텐츠에 대한 서명으로 인증을 통한 신뢰 구축 가능

• 기존 네트워크 공격에 대한 대응 제공
- 동일한 다중 Interest Packet에도 오직 한번의 Data Packet 만 응답함
- 주소기반이 아닌 Named 기반이기 때문에 정확한 Content Name이 필요함
- 보안 서명이 필수이기 때문에 Data Packet이 노출된다고 해도 보안상 안전
- DoS, DDoS, Sniffing, Man-in-the-middle-Attack, Reflection Attack 등 예방

• NDN 네트워크에 대한 공격 대응 제공
- Interest flooding 공격: 동일한 Interest Packet에 대하여, 요청한 데이터와 동일한 Data Packet을 가지고 있는 인접한 라우터가 오직 한번만 응답함
- Data flooding 공격: 자주 요청되는 Data는 Consumer 인접 라우터에서 응답하고, 오직 인접 라우터에 없는 데이터만 응답함

3.2 MobilityFirst 보안기술 분석

MobilityFirst 프로젝트는 현재 인터넷의 설계 원칙인 유연성과 적용성, 보안성은 많은 변화를 가져왔으나, 현재 사용자와 사용자 단말은 끊김 없이(seamless) 통신에 대한 요구와 수요가 증가하고 이를 위한 고정 엔드 포인트(fixed end-point) 간의 통신을 지원하기에는 기존의 인터넷의 한계가 발생하게 되었기 때문에 이를 해결하기 위하여 이동성(Mobility)를 기본으로 하는 구조를 개발하기 위한 방안을 제시하기 위한 프로젝트이다. 통신 채널을 설정하기 위하여, 사용자 단말이 이동되는 것을 예외적인 사항으로 규정하지 않고, 근본적으로 단말이 이동되는 것을 고려하여 네트워크 구조를 설계하고, 사용자의 이동으로 인하여 통신채널의 연결이 단절되었을 때도 데이터의 전송을 보장하는 GDTN(Generalized Delay-Tolerant Network)를 기초로 하는 네트워크를 설계하고자 한다. 또한 자기 인증(self-certifying) 기능을 수행하는 공용 어드레스를 이용하여 네트워크의 신뢰성을 높이고자 한다. 이러한 구조는 contextaware 서비스 또는 location-aware 서비스를 보장하는 것을 목표로 하고 있으며, MobilityFirst 프로젝트는 사용자 단말의 이동성 지원과 네트워크의 확장성 및 가용성 측면에서의 균형(trade-off), 그리고 이동 단말 간의 효율적인 통신 구조 설계를 목표로 한다 [25].

3.3 Nebula 보안기술 분석

Nebula는 라틴어로 클라우드(cloud), 사전적 의미로는 성운을 의미한다. 즉, Nebula 프로젝트는 클라우드 중심의 미래인터넷 구조 연구를 수행하는 프로젝트이다. 이는 데이터의 저장, 컴퓨팅, 애플리케이션을 클라우드 시스템으로 통합하는 형태로 새로운 인터넷 환경은 신속한 통신 자원을 제공하고, 유틸리티 형 과금 방식 및 일관적이고 용이한 관리 등이 가능한 네트워크 중심의 글로벌 컴퓨팅 인프라 구축을 요구하고 있다.

이를 위하여, 사용자는 클라우드에 접속할 수 있는 단말만 구비하고, 처리되는 데이터의 저장 및 컴퓨팅은 데이터 센터로 구성되는 클라우드에서 수행하게 된다. 이러한 클라우드 환경의 중심에는 데이터 센터가 중요한 요소이며, 클라우드 컴퓨팅 데이터 센터는 사용자와 데이터 간, 데이터 센터들 간의 신뢰성과 보안성이 매우 높고, 확장이 가능한 네트워크의 설계는 해결해야 할 과제 이다.

이러한 과제 해결을 위하여 Nebula는 신뢰성 있는 데이터 및 컨트롤 시스템과 코어 라우터 간의 병렬 경로 구축 등의 네트워킹 방식을 개발함으로써, 인증 메커니즘에 기초한 통신 채널을 구축하여 언제나 이용 가능한 네트워크 서비스를 제공하는 클라우드 컴퓨팅

모델을 지원하는 것을 목표로 하고 있다. 또한 클라우드 아키텍처의 구축 과정에 영향을 미치는 기술적이 문제들의 해결 방안에 대한 연구를 진행하는 프로젝트이다. Nebula의 보안 기능은 신뢰성, 시스템 접근에 대한 기밀성, 무결성 및 가용성 등의 보안기능에 대하여 논하고 있다.

NEBULA의 보안기능의 분석은 3가지 측면으로 분석된다. 안전한 데이터 센터, NDP(Nebula Data Plane)와 NVENT(Nebula virtual and Extensible Network Techniques)를 통한 보안성 향상, clustering 컴퓨팅과 NCore(Nebula Core)를 통한 보안성 보장으로 설명될 수 있다 [30].

- 안전한 데이터 센터
  - 클라우드를 통한 데이터의 무결성, 안전성, 보안성, 신뢰성 확보
  - 안전한 보안체계를 기반으로 데이터의 접근성과 효율성이 높아짐
  - 다중 클라우드 데이터 센터를 통한 신속한 서비스 제공과 업그레이드용이
  - 그러나 이를 실현하기 위해서는 클라우드 컴퓨팅이 안전하고 신뢰성이 높다는 기본 전제가 요구됨
- NDP와 NVENT를 통한 보안성 향상
  - 다양한 보안 정책을 통한 패킷(데이터)에 대한 신뢰성 및 보안성 향상
  - 미래 인터넷을 대비한 다양한 정책과 기술이 적용될 수 있도록 확장성 제공
  - 인증, 허가, 무결성, 기밀성을 제공하고 보장
- 클러스터링 컴퓨팅과 NCore를 통한 보안성 보장
  - 클러스터링 컴퓨팅과 라우터의 병렬연결과 처리를 통한 보안성 보장
  - 병렬 구성을 통한 장애 처리 및 대처와 업그레이드가 용이
  - 지능적인 라우터 소프트웨어를 통한 보안 네트워크 구축이 용이
  - 미래 인터넷에 대비 한 보안 구성과 확장이 용이

3.4 XIA 보안기술 분석

XIA(eXpressive Internet Architecture)는 미국의 NSF가 2010년부터 시작한 FIA(Future Internet Architecture) 프로그램 중 네 번째 섹션인 XIA 프로젝트는 카네기멜론 대학 등이 참여하여 보안성 중심의 미래형 네트워크를 연구하고 있다. 보안성은 다양한 미래 네트워크연구의 필수적인 요구사항이지만, XIA 프로젝트는 네트워크계층 내부에서 본질적으로 제공하는 보안성(Built-In Security)을 목표로 하여 네트워크 구조 연구를 진행 중 이다.

XIA프로젝트에서는 다양한 통신개체(예, 호스트, 서비스, 콘텐츠 등)를 지정하고, 통신 개체들 간의 인증 및 전달되는 콘텐츠의 무결성(신뢰통신)을 제공하는 네트워크 구조에 대한 보안성 중심의 네트워크 구조에 대한 연구 분야이다.

현재 인터넷 설계 당시 보안적인 측면에 대하여 설계가 고려되지 않았다. 즉, 현재의 IP계층은 패킷의 전달 기능만 담당하고 사용자 인증 및 전달되는 데이터의 무결성, 데이터의 보호를 위한 암호화 기능은 애플리케이션 영역에서 담당하도록 설계되어 있다.

XIA는 유연성(Flexibility)을 기본 구조로 우리가 예측할 수 없는 방법으로 확장이 가능하다. XIA의 보안은 근본적인 구조, principals type(형태)과 메커니즘의 확장성 등에 달려있다. XIA의 주요 보안 요소는 다음과 같다.

- Availability(유효성): host 와 service 통신의 유용성을 보장하고, 인접 콘텐트와 서비스들을 찾는 문제, DoS 공격에 대하여 안전
- Authenticity / Integrity: User, host, domain, Service, content 의 인증(self-certifying을 사용하기 때문에)
- Authentication and Accountability: Authorization(허가)와 deterrence(제지)를 보장
- Identity 보호, anonymity(익명성), 프라이버시: 패킷을 sender와 receiver가 원하는 경우 프라이버시 보호
- 신뢰적인 관리의 유연성

XIA에 사용하고 있는 보안관련 기술은 다음과 같이 정의된다.

- 다양한 principal 유형들: 자율적인 도메인(domains) 범위를 허용하고, 계층구조를 가지고 있음.
- 근본적인 보안 식별자(identity): self-certifying 또

는 self-verifiable 식별자의 사용으로 ID를 한번 알게 되면 보안을 보장함. 외부의 설정에 의존할 필요가 없기 때문에 principal ID는 “human ID” 와 “intrinsic ID” 의 다리 역할.

- 유연한 신뢰의 관리: 네임 리솔루션을 사용하고, 통신 엔티티 간의 부트 트래핑(boot trapping)을 신뢰, 신뢰관리를 위한 많은 자원을 지원.

XIA에서의 보안은 현재 구조인 narrow waist 구조를 그대로 적용하여 IP 계층은 패킷 전달의 기능만을 담당하고, 사용자의 인증 및 전달되는 데이터의 무결성, 데이터 보호를 위한 암호화 기능은 애플리케이션 영역에서 담당하여 보안의 기능을 네트워크 계층에서 원천적으로 수행하도록 하기 위한 연구가 아직 진행중에 있다 [29].

4. 미래인터넷을 위한 신뢰통신 연구

현재 미래인터넷에 대한 청사진은 아직 많은 부분이 미정인 상태로 놓여 있으며, 그 속에 미래인터넷의 보안에 대한 측면 또한 전면에 드러나고 있지 못하고 있는 실정이다. 현재 미래인터넷 설계에 있어서 특징점들로 스마트(smart)형 인터넷서비스, 유비쿼터스형 인터넷서비스, 그린(green)형 인터넷서비스, 안전(safety)형 인터넷서비스, 실감(realistic)형 인터넷서비스 등으로 미래인터넷 특징을 요약하고 있지만, 이 역시, 미래인터넷이 예측해야하는 환경과 보안에 대한 고민은 아직 해결되지 있지 못하다.

본 논문에서 분석한 FIA 프로젝트에서도 역시 미래인터넷 보안적인 측면에 대해 기술· 정책적인 접근에 대한 구체적인 방향 제시는 현재까지는 논의 되지 않고 있다.

본 장에서는 미래인터넷 보안을 위해서는 신뢰할 수 있는 통신을 위한 기법의 필요성과 연구방향으로 다음과 같이 제언한다. 미래인터넷상에서 복수의 이종간의 통신에서 가장 고려되어야 할 사항은 이종간의 안전하고 상호간 신뢰할 수 있는 통신 인프라가 구축되어 있어야 하는 것과 이런 안전한 통신 인프라를 기반으로 이종간 상호 인증할 수 있는 통합 인증 시스템이 구축되어 있어야 한다.

다시 말해 미래 인터넷 기술에서 가장 중요시되고 핵심적으로 접근해서 연구해야 할 기술은 이종간의 안전한 신뢰 통신이 이루어질 수 있도록 하는 신뢰 통신 기술을 연구하는 것과 안전한 신뢰 통신을 기반으로 이종간 상호 인증할 수 있는 통합 인증 기술을 연구하는 것이다.

미래인터넷은 복수의 이종네트워크와 호스트, 콘텐츠, 클라우드 컴퓨팅 가상화 등 다양한 신뢰통신 대상간의 효율적이고 공통적용이 가능한 신뢰통신 기법을 요구하고 있다. 이러한 보안요구사항을 만족하기 위해 선행 연구로 이루어져야하는 부분이 신뢰통신 참조 모델 즉, 통합인증을 포함하여 수용하는 과정에서 여러가지 미래인터넷 요구사항을 만족하는지 검증하기 위한 기술 및 프로세스 연구가 필요할 것이다. 참조모델을 위한 기술은 기능적인 구성요소와 인터페이스를 이해하기 위한 개념적 프레임 워크를 제공해야한다. 또한 이를 위해 지적 배경(intelligential context)을 제공하고 또한 지속적인 연구와 개발이 지속적으로 진행되어야 할 것이다.

이를 위해 신뢰통신 기반의 기술 개발에 있어서 미래인터넷 신뢰통신 참조 모델 검증 기술에 대한 지속적인 연구가 필요할 것이다.

5. 결 론

새로운 패러다임인 미래인터넷의 원천 기술의 확보와 글로벌 시장의 선점을 위해서는 미래인터넷을 IT 인프라 분야의 확보를 위한 산업과 연계한 연구개발 전략 등의 기본계획을 수립하여 통합관리의 추진 체계가 절실히 필요하다. 이를 위하여 신뢰할 수 있는 통신을 위한 미래인터넷의 보안에 대한 중요성을 인식하고 그 보안기능에 대한 분석이 선행되어야할 것이다.

이에 본 논문에서는 보안기술에 대한 보안기능분석과 미래인터넷을 위한 신뢰통신의 필요성과 연구방향에 대하여 제안하고 기술하였다. 향후 연구 방향은 이를 기반으로 세계적으로 우리나라가 우위에 설 수 있는 보다 나은 미래인터넷의 보안기능 설계와 구축을 위한 통합구축 시스템에 대한 연구가 지속되어져야 할 것이다.

참고문헌

[1] 김대영, “미래인터넷 개념 및 현황”, 인터넷 미래기술, 2010.3.

[2] 김성수, 최미정, 홍원기, “미래 인터넷 연구 동향과 관리기능 정의”, KNOM 2008, 2008.4.

[3] 김영화, “미래인터넷의 네트워크 가상화 기술 동향”, 전자통신동향분석 제25권 제1호, 2010.2.

[4] 김진년, 이경민, 김춘희, 차영욱, “미래 인터넷을 위한 ICT 자원 가상화의 제어 프레임 워크”, 한국정보보호학술논문지, 제 9권 제 10호, 2011.10.

[5] 백은경 외, 미래 네트워크 기술 동향, 주간기술동향 1387호, 2008.3.

[6] 변성혁, “미래인터넷 아키텍처 연구동향”, 전자통신동향분석 제24권 제3호, 2009.6.

[7] 서동일, 이상호, “1.25 인터넷 침해사고의 분석과 대책”, 대한전자공학회지, 제30권 제6호 pp. 49~57, 2003.

[8] 서동일, 정종수, 조현숙, “미래인터넷 정보보호 요구사항”, 인터넷정보학회지, 제 10권 제4호, pp. 9-79, 2009.

[9] 신명기, “미래인터넷 기술 및 표준화 동향”, 전자통신동향분석, 제22권 제6호, 2007.

[10] 서동일, 정종수, 조현숙, “미래인터넷 정보보호 요구사항”, 인터넷정보학회지, 제 10권 제4호, pp. 9-79, 2009

[11] 유태완, 한영희, 이혁준, 김대영, 고석주, 신명기, 정희영, “미래 인터넷을 위한 네이밍과 어드레싱을 위한 연구”, 정보과학회지, 2011.3.

[12] 이상우 외, “미래인터넷 보안기술 동향”, 전자통신동향분석, 제 26권 제5호, 2011.10.

[13] 조기덕, 박건우, 이문영, “미래 컨텐츠 네트워크 연구 동향 분석”, 미래인터넷 포럼 이슈 분석 시리즈, 제 12호, 2010.12.

[14] “미래인터넷 보안기술 및 정보보호 등에 대한 이슈 및 개발 수요 조사”, 한국인터넷 진흥원 연구보고서, 2010.11.

[15] “미래 인터넷 국가별 추진동향 분석 및 연구”, 한국인터넷진흥원 연구 보고서, 2010.11.

[16] Dong-il Seo, "Security Considerations for the Future Internet", FIWC 2010, February 2010.

[17] FIND, http://find.isi.edu

[18] FN2020 포럼. http://www.fn2020.or.kr

[19] FP7, ICT, network of the future, http://cordis.europa.eu/fp7/ict/future-networks

[20] Future Internet Assembly. http://www.futureinter.net.

[21] GENI, http://www.geni.net

[22] GENI, Spiral 2 Overview, GENI Project Office, 2010.06.

[23] ITU-T X.805, "Security architecture for systems providing end-to-end Communications", 2003.

[24] ITU-T Y.2701, "Security Requirements for NGN Release 1", 2008.

[25] MobilityFirst,http://mobilityfirst.winlab.rutgers.edu/

[26] NDN, http://www.named data.net/

[27] NSF, Future Internet Architecture Project.

[28] David Clark et al., “New Arch: Future Generation Internet Architecture Project Final TechnicalReport”, http://www.isi.edu/newarch/, 2003.

[29] XIA, eXpressive Internet Architecture Project. http: //www.cs.cmu.edu/~xia

[30] Tom Anderson et al.,, “NEBULA - A Future Internet That Supports Trustworthy Cloud Computing,”, Collaborative Research.

[저 자 소 개]

전 은 아 (Eun-A Jun)

1999년 2월 원광대 전자재료공학과 학사
2001년 8월 원광대 전자계산교육학 석사
2011년 8월 고려대학교 정보보호대학원 (정보보호 전공) 박사
2011년 9월~현재 고려대 정보보호연구원 연구교수

email : eajun@korea.ac.kr

서 동 일 (Seo, Dong-il)

1989년 2월 경북대 전자공학과 졸업
1994년 2월 포항공대 정보통신과 석사
2004년 8월 충북대 전산학과 박사
1994년 3월~현재 한국전자통신연구원 팀장(책임연구원)
2010년 3월 ~ 현재 : 충남대학교 겸임교수

email:bluesea@etri.re.kr

이 도 건 (Do-geon Lee)

2007년 2월 남서울대학 학사
2010년 2월 고려대 정보보호대학원 석사
2009년 3월 ~ 2010년 6월 경기대학교 산업기술보호특화센터 전임연구원
2012년 01 ~ 현재 금융결제원 금융정보보호부

email : dogeonLee@kftc.or.kr

김 점 구 (Jeom goo Kim)

1990년 2월 광운대 전자계산학과 이학사
1997년 8월 광운대 전자계산학과 석사
2000년 8월 한남대 컴퓨터공학 박사
1999년 3월~현재 남서울대학교 컴퓨터학과 정교수

email : jgoo@nsu.ac.kr

이 상 우(Lee, Sang-Woo)

1999년 2월 경북대 전자공학과 학사
2001년 2월 경북대 전자공학과 석사
2009년 2월 경북대 전자공학과 박사
2001년 1월~현재 한국전자통신연구원 사이버융합보안연구단 선임연구원

email : ttomlee@etri.re.kr