미래인터넷 정보보호 요구사항

서 동 일* 장 종 수** 조 현 숙***

◈ 목 차 ◈

1. 서 론

향후 미래 사회의 상호 작용은 유비쿼터스 환경으로 이루어질 것이며, 이의 기반을 이룰 네트워크는 인터넷(Internet)일 것으로 예측되고 있다. 유비쿼터스 환경이란 언제(any time), 어디서나(any where), 어떠한 통신 매체(any media)를 사용하던지 통신 네트워크에 접근이 가능하게 되는 환경을 이야기 한다. 또한, 유비쿼터스 환경에서는 사용자의 위치를 파악하고 현재 처해있는 상황에 맞게 적절한 서비스를 제공해 주게 된다. 이러한 적절한 서비스를 제공하기 위해서는 스스로 판단하여 행동할 수 있는 단말 에이전트들이 필요하게 된다.

현재의 인터넷은 1969년에 구축이 시작된 ARPANET에서 출발하여, 1974년 인터넷의 기본 개념이 제안되고 1978년 TCP/IP 프로토콜이 설계되면서 시작되었다고 볼 수 있다. 그러나, 현재의 인터넷은 최초 설계 시 무선/이동성(mobility, wireless), 보안성(security) 등이 고려되지 않아 여러 가지 한계점을 내포하고 있다. 예를 들어, 유비쿼터스 환경 구현에 그대로 활용하기에는 현재의 인터넷 접속은 제약사항이 많으며, 일반인의 인터넷 사용이 무제한적으로 허용되지도 않는다. 인터넷을 통해 다양한 매체로의 데이터 전송이 일부 가능하지만, 무선인터넷을 활용한 끊김 없는 전송에는 제약이 있다. 인터넷 접속을 위한 다양한 기기들이 존재하지만 이들 기기간 상호 통신이 원활하지 않으며, 콘텐츠의 공통 이용에도 불편하다. 인터넷에서의 보안 문제는 거의 대부분 사후 조치 형태이며 예방이 쉽지 않다. 인터넷 관련 응용 소프트웨어는 전문적인 지식이 없는 일반인이 사용하기에 아직까지는 이해하기가 어렵다[18].

이러한 문제의식에서 출발하여 미국, EU, 일본 등 주요 선진국은 현 인터넷의 한계를 해결하고 전송품질의 보장, 이동성, 완벽한 보안 및 새로운 융합서비스를 확장·수용할 수 있는 개념의 미래인터넷(Future Internet) 연구개발 프로그램을 정부 주도로 추진 중에 있으며, 미래 인터넷을 세계적인 경기침체 및 경쟁, 기후변화, 노령 인구 증가 등 국제적인 도전과제에 대한 하나의 해결책으로까지 제시하고 있다. 이를 위해 미국에서는 NSF(미국과학재단) 주도하에 미래 인터넷을 설계하고 시험하기 위한 FIND(Future Internet Design), GENI(Global Environment for Network Innovations) 프로젝트가 수행되고 있으며, 유럽이나 일본에서도 관련된 프로젝트가 성립되어 연구되고 있는 실정이다. 국내의 경우에도 미래인터넷 관련 연구가 2007년부터 점진적으로 수행되고 있다[12,13,14,18].

본 기고문에서는 2장에서 미래인터넷이 등장하게 된 기존 인터넷의 문제점과 새로운 미래 융합서비스

* 한국전자통신연구원 지식정보보안연구부 팀장
** 한국전자통신연구원 지식정보보안연구부 책임연구원
*** 한국전자통신연구원 지식정보보안연구부 부장

등에 대해 알아보며, 3장에서 미래인터넷 환경에서의 보안 위협 요소 및 대응방안을 살펴본다. 4장에서는 이러한 미래인터넷 구현을 위한 정보보호 요구사항을 알아보고, 마지막으로 5장에서 결론 및 향후 연구내용에 대하여 기술한다.

2. 미래인터넷의 등장

2.1. 미래 인터넷 요구의 등장

현재까지 알려진 미래인터넷의 정의는 “현재 인터넷 구조의 한계성을 극복하고 미래의 새로운 요구사항을 수용하기 위해, 기존 인터넷과의 호환성을 필수조건으로 고려하지 않는 혁신적인 개념(clean-slage)으로 설계될 미래의 새로운 인터넷”이라고 한다. 이러한 정의에서 알 수 있듯이 미래 인터넷의 등장은 현재 인터넷 성장의 한계성을 극복하기 위한 점, 미래의 새로운 요구사항을 수용하기 위한 점이라는 두가지 조건을 만족시키기 위해 시작되었다고 볼 수 있다.

현재 인터넷이 제안될 당시 기본적인 설계 철학은 아래와 같은 다섯가지 개념을 가지고 시작되었다.

- 계층화(Layering)
- 패킷 스위칭 (packet switching)
- 네트워크의 네트워크
- 네트워크의 단순화 및 단말의 지능화
- 단대단 통신(end-to-end argument)

그러나, 오늘날의 인터넷 환경에서는 위와 같은 개념들이 위협받고 있는 상황이며, 인터넷의 눈부신 성장이 오히려 인터넷에 위기를 불러오고 있는 형편이다. 과거, 소수의 서로 믿을 수 있는 연구자들이 그들이 가진 호스트를 서로 연결하여 데이터를 상호 공유하는 것을 전제로 설계된 현재의 인터넷이 이동하는 많은 사용자들이 다양한 컨텐츠를 활용하기 위한 기반으로 쓰이게 됨에 따라 원래는 예상하지 못했던 문제들이 드러나고 있는 것이다. 예를 들어, 매우 높은 수준의 트래픽 부하, 실시간 비디오 전송, 개별 노드 또는 서브 네트워크의 이동성, 무선 채널의 일시적이고 우연적인 연결성, 위성이나 자동차간 연결과 같은 링크의 특성 문제, 긴 지연시간을 갖는 연결, 간헐적으로만 연결되어 있는 링크 등이 새로운 문제점으로 나타나고 있는 것이다. 이러한 한계를 극복하기 위한 임시적 해결책은 오히려 더 큰 문제를 야기하고 있다. 예를 들어, 인터넷주소 변환장비(NAT), 방화벽, 로드 밸런서(Load Balancer)등은 주소 자원의 부족, 보안성, 트래픽 분산 등의 효과를 가져왔지만 반대로 종단간 투명성(end-to-end transparency)을 깨뜨림으로써 오히려 새로운 발전을 저해하는 요소가 되고 있다. 또한, 패킷 스위칭은 테라바이트와 같은 초고속 통신에는 오히려 성능을 떨어뜨리는 한 요소가 되고 있으며, 계층화는 보안 문제를 해결하기 곤란하게 만드는 요소가 되고 있다.

또 하나의 미래 인터넷 등장 배경에는 현재의 인터넷에서 제공하기에 매우 어려운 새로운 융복합 서비스의 요구사항 때문이다. 예를 들어, 사용자가 언제 어디서나 어떠한 매체를 활용하여서도 본인이 원하는 네트워크 서비스를 제공 받기를 요구한다는 점, 사용자가 별도로 지정하지 않더래도 현재의 상황을 네트워크가 스스로 인지하여 그 상황에 맞는 서비스를 제공할 수 있어야 한다는 점 등이다. 이러한 서비스들은 기본적으로 유비쿼터스 환경이 구축되어 있어야 하며, 이의 근간을 인터넷에서 제공할 수 있게 하기 위해서는 지금의 인터넷과는 다른 새로운 인터넷이 필요하게 된 것이다.

(그림 1) 미래인터넷 요구사항(요약)

또한, 사용자들은 그들의 눈에 보이지 않으면서도

동시에 사용자가 무엇을 사용하고 있다는 사실조차 알 필요가 없이 고도화된 서비스 제공을 요청하고 있으며, 이를 위해서는 주변의 모든 사물을 무선 네트워크로 연결하여야 하고 다른 한편으로는 이러한 서비스나 사물을 사용자의 시선을 끌지 않고 자연스럽게 조합할 수 있어야 한다. 이러한 요구 사항은 현재 우리가 사용하고 있는 네트워크(인터넷) 구조로는 지원하기 불가능하거나 효율적인 구현이 어려우며, 따라서 새로운 인터넷 즉, 미래 인터넷이 요구되게 된 것이다.

이와 같이 미래 인터넷이 필요로 하게 되는 사용자들의 일반적인 요구사항은 크게 현재 인터넷이 가지고 있는 문제점과 미래 융복합 서비스의 신규 요청사항이 복합적으로 작용되어 제시되고 있으며, 이들을 요약하면 (그림 1)과 같다.

2.2. 미래 인터넷 서비스 기술의 특징

미래 인터넷 서비스 기술은 데이터 중심, 호스트 중심인 현재의 인터넷 서비스 기술과는 다르게 데이터 및 콘텐츠 중심의 네트워킹 서비스, 사용자 중심의 네트워킹 서비스를 제공할 것으로 보인다.

사용자 중심의 네트워킹 서비스 기술은 사용자의 상황에 따라 적절한 서비스를 제공하는 것으로서, 기존의 인터넷 상황에서는 매우 어려운 서비스이다. 이를 위해서는 사용자의 상황을 인지할 수 있는 단말이 필요하게 되며, 사용자의 상황 변화에 따라 가장 최적의 서비스를 제공할 수 있도록 여러 가지 적절한 동작(예를 들어, 기존의 연결을 종료하고 새로운 연결을 설정한다 든지 하는 동작)을 수행하는 새로운 응용 프로그램이 필요할 것이다. 또한, 네트워크 자체도 사용자의 상황에 따라 적절한 가상의 네트워크 연결을 제공할 수 있어야 하며, 정보보호 기능 또한 이러한 연결 상태에 따라 적절한 서비스가 제공될 수 있어야 한다. 따라서, 사용자 중심의 네트워킹 서비스 기술을 제공하기 위해서는 상황인지 단말, 상황에 맞는 네트워크 재구성 기술, 상황에 따른 정보보호 서비스 제공 기술 등이 필수적으로 필요하게 될 것이다.

미래인터넷에서는 기존의 호스트 중심의 서비스가 데이터 및 콘텐츠 중심의 네트워킹 서비스로 변화될 것이다. 이는 현재 전체 인터넷 트래픽의 대다수를 웹 서비스가 차지하고 있다는 점에 기인한다. 즉, 이전의 호스트간 연결은 미래 인터넷 환경에서는 별 의미가 없으며, 특정한 데이터나 콘텐츠를 서비스 받기 위한 인터넷 접속이 주류를 차지할 것이다.

따라서, 특정 호스트 간의 연결을 만들고 유지하는 것 보다는 필요한 데이터 및 콘텐츠를 찾아서 받아오는 것을 중심으로 네트워크가 동작하는 즉, 데이터 및 콘텐츠 중심의 네트워킹 서비스가 필요하게 될 것이다. 이를 위해 다대다 혹은 에니캐스트(Anycast) 방식의 통신 형태가 주류를 차지하게 될 것이며, 특히 기존의 인터넷에서는 주소가 바뀌지 않고 매우 안정적으로 운영되는 호스트가 매우 중요하였으나, 미래 인터넷 환경에서는 모바일 디바이스와 같은 수시로 바뀔 수 있는 네트워크 구성 형태에서 호스트 자체는 중요하지 않으며 사용자가 원하는 데이터 및 콘텐츠를 중심으로 하는 네트워킹 서비스가 중요하게 고려될 것이다.

3. 미래인터넷의 위협요소와 대응

현재 인터넷에 위협이 되는 여러 가지 악성코드라든지 인증의 문제 같은 것들은 미래 인터넷에서도 여전히 위협요소로 나타날 것으로 보인다. 이러한 항목들에 대해 몇가지 주요 이슈별로 살펴보면 아래와 같다.

현재 사용자 인증의 방법으로 가장 널리 사용되는 방법은 아이디와 패스워드를 사용하는 방법이다. 그러나 이러한 방법은 인터넷 사용의 확대와 함께 관리해야 하는 아이디와 패스워드가 늘어나면서 어려움을 가지고 있으며, 현재의 인터넷 환경에서도 이를 해결하기 위한 여러 가지 기술적 방법들이 나타나고 있다. 그러나, 미래 인터넷 환경에서는 상황과 수준에 맞는 정보보호 기능을 제공하기 위해서 현재와 같은 단순한 형태의 인증 방법은 미흡할 것으로 보이며, 새로운 형태의 사용자 인증 메커니즘이 필요할 것으로 보인다.

다음으로 악성코드에 대한 위협을 살펴보면, 현재와 같은 악성코드에 의한 인터넷 위협은 지속적으로 그리고 더욱 더 확대되어 나타날 것으로 보인다. 최근 인터넷을 공격하는 해커들은 금전적인 이익을 위해

해킹하는 사례가 늘어나고 있는 실정이며, 이러한 범죄에 가장 많이 활용되는 공격은 악성코드를 활용한 위협이다. 또한, 인터넷을 활용한 사기 기법도 기존의 단순한 개인정보를 활용하던 수준에서 벗어나 자동화된 메커니즘을 활용하는 수준으로 고도화될 것으로 보인다.

현재와 같은 인터넷 프로토콜에서는 네트워크에 송수신되고 있는 패킷을 가로채서 스팸, 서비스거부공격 등과 같은 보안 위협을 야기할 수 있다. 더욱이 패킷의 원본 주소를 속일 수 있기 때문에 이를 활용한 보안 위협은 매우 높은 수준이며, 이러한 문제를 해결하기 위한 메커니즘 또한 미래 인터넷에서는 필수 불가결한 요소일 것이다.

현재의 인터넷에서 가장 기본적인 인터넷 서비스인 DNS(Domain Name Service)는 지금도 안전하지 못하며, 이를 공격한 대표적인 사례가 1.25 인터넷 침해사고이다[11]. 따라서, 미래 인터넷에서는 이를 대체할 새로운 프로토콜 혹은 지금과 같은 형태의 서비스를 활용할 때 나타날 수 있는 보안 위협에 대해서 더욱 더 강하고 안전한 메커니즘을 제공하여야 할 것이다.

미래 인터넷 환경에서 대표적인 PC 대체 기기로는 스마트폰이 있다. 특히, 미래사회의 근간이 유비쿼터스 환경이라고 볼 때 이를 지원하는 대표적인 단말기기로 스마트폰이 유력하게 떠오르고 있다는 점을 고려하여야 한다. 스마트폰은 음성통화, 무선인터넷과 같은 휴대폰 기본 기능을 지원함과 동시에 모바일 환경에서 여러 가지 다양한 기능(음악, 영화, 카메라, 위치확인 서비스, 개인일정 관리, e-mail 등)을 수행할 수 있는 일종의 모바일 PC 플랫폼이라고 볼 수 있다. 그러나, 이렇게 다양한 기능을 수행하는 스마트폰은 기본적으로 인터넷을 활용하고 있는 PC에서 발생할 수 있는 모든 보안 위협이 동일하게 적용될 수 있다는 위험이 존재한다. 더욱이 중요한 개인정보가 스마트폰에 저장되어 있으며, 개방적인 개발 환경으로 인해 악성코드의 제작과 유포가 손쉽게 이루어질 수 있다는 위험성이 상존하고 있다. 따라서 미래 인터넷 환경에서는 이러한 문제들을 방지하기 위한 메커니즘과 디바이스 보안 방법이 필수적일 것으로 보인다.

미래 인터넷은 매우 중요한 시스템(예를 들어, 국가 기간산업, 금융망 등)과 네트워킹되어 동작될 가능성이 크며, 이러한 시스템은 그 중요성에 비추어 지금까지의 보안 위협과는 차원이 다른 중요도로 나타날 가능성이 높다. 따라서, 이러한 크리티컬한 시스템에 대한 보안 위협에도 대처할 수 있는 방안 역시 미래 인터넷 환경에서는 고려되어야 할 것이다.

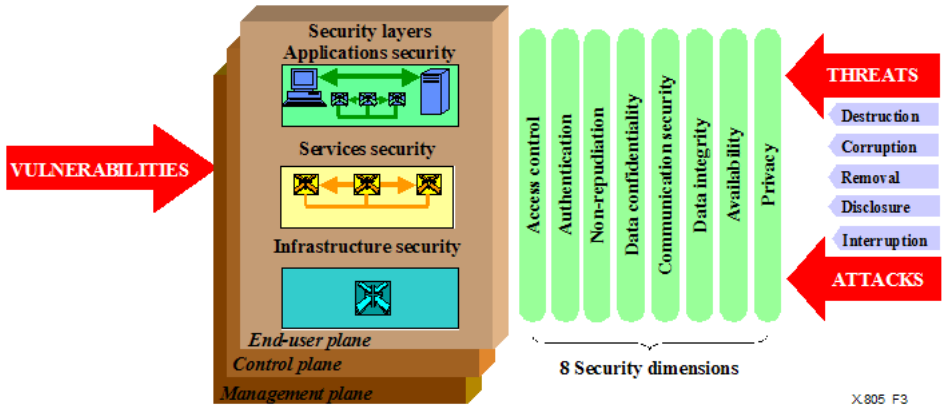
이러한 여러 가지 미래 인터넷 환경에서의 보안 위협에 대처하기 위한 하나의 방법으로 미래 인터넷에서 사용되는 모든 프로토콜에 대해 인증 메커니즘과 필터링 기능을 지원하게 하는 방법도 고려해 볼 수 있을 것이다.

4. 정보보호 요구사항

앞 장에서 살펴본 미래인터넷의 위협 요소를 반영한 미래인터넷 정보보호 요구사항에는 여러 가지 사항들이 있을 수 있다.

특히나 미래인터넷에서의 정보보호 기능은 사용자들에게 적절한 수준별 정보보호 기능을 지원하기 위해서 매우 다양한 형태로 구현될 필요가 있을 것이다. 예를 들어, 사용자가 원하는 서비스가 신뢰를 기반으로 해야 될 서비스로써 높은 수준의 정보보호를 원하는 지 아니면 제공하는 기능에 중심을 둔 저 수준의 정보보호를 원하는 지에 따라서 매우 다양하게 나타나게 될 것이다. 이를 그림으로 표현하면 (그림 2)와 같다. 즉, 정보보호에 무게중심을 둘 것인지 아니면 서비스의 제공에 중심을 둘 것인지에 따라 제공되는 정보보호의 강도가 달라질 것이다.

(그림 2) 정보보호 vs. 개방성



Security architecture for end-to-end network security

(그림 3) 종단간 네트워크 정보보호 구조 (ITU-T X.805)

ITU-T에서는 미래 네트워크에서 고려하여야 할 정보보호 요구사항을 규정한 바 있으며, X.805 권고안에서 종단간 네트워크 정보보호를 위한 구조로서 (그림 3)을 권고하고 있다. 이를 보면, 사용자의 종단간 통신 접속을 위협할 수 있는 여러 가지 요인들에 대해서 (예를 들어, Destruction, Corruption, Removal, Disclosure, Interruption 등) 아래와 같은 8가지 측면의 정보보호 기능을 제공해야 한다고 되어 있다. 이러한 정보보호 기능은 사용자평면(user plane), 제어평면(control plane), 관리평면(management plane)에 각각 적합하도록 적응되어 제공될 수 있어야 한다[9].

- 접근제어(Access control)
- 인증(Authentication)
- 부인봉쇄(Non-repudiation)
- 데이터 기밀성(Data confidentiality)
- 통신보안(Communication security)
- 데이터 무결성(Data integrity)
- 가용성(Availability)
- 프라이버시(Privacy)

또한, ITU-T Y.2701 권고안에서는 이러한 8가지 정보보호 기능에 대해서 차세대네트워크(NGN, Next Generation Network)에서 제공하여야 할 기능으로 아래와 같이 권고하고 있다[10].

- Access Control : 인증된 가입자에게만 접속을 허용하여야 한다. 인증된 가입자로 위장하여 침입하는 것과 같은 비인증된 가입자에 대해 적절한 방어책을 가지고 있어야 한다.
- Authentication : 인증하여야 할 가입자, 장비, 네트워크 요소 등에 대해서 적절히 인증해 줄 수 있는 능력을 가지고 있어야 한다.
- Non-reputation : 부인봉쇄에 대해서는 특정하지 않고 있다.
- Data Confidentiality : 암호나 다른 수단에 의해서 가입자의 트래픽에 대해 기밀성을 제공할 수 있어야 한다. 이러한 기능은 제어 메시지나 관리 트래픽에 대해서도 동일하다.
- Communication Security : 정보를 불법적으로 가로채거나 전용하는 것을 방지할 수 있는 메커니즘을 제공하여야 한다.
- Data integrity : 암호나 다른 수단에 의해서 가입자의 트래픽에 대해 무결성을 제공할 수 있어야 한다. 이러한 기능은 제어 메시지나 관리 트래픽에 대해서도 동일하다.
- Availability : 서비스거부공격, 바이러스 및 웜 등의 유포 등과 같은 악성코드의 공격을 차단하거나 방어할 수 있는 능력을 제공하여야 한다. 내부 네트워크 요소들은 바이러스, 웜, 기타 다른 공격 들을 신속하게 탐지할 수 있어야 한다. 정보보호 정책에 위반되는 패킷이나 트래픽을 필터링할 수 있는 능력을 가지고 있어야 한다. 재난에 대비한 복구 기능 및 절차를 지원할 수 있어

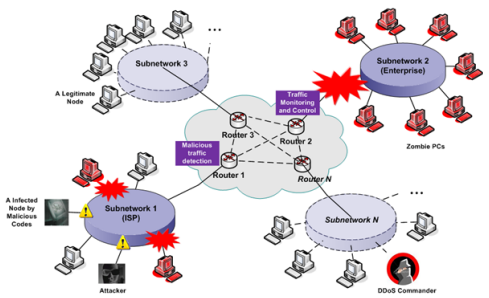
야 한다.

- Privacy : 가입자의 위치정보, ID정보, 전화번호, 네트워크 주소 등과 같은 가입자의 프라이버시 정보를 보호할 수 있는 능력을 가지고 있어야 한다.

아직까지 미래 인터넷 정보보호 기능에 대해서는 뚜렷한 해결책과 요구사항 등이 연구되어 있지 않다. 따라서, 위와 같은 ITU-T 권고안 정보들은 미래 인터넷을 설계할 때 참조할 수 있는 좋은 정보들일 것이다.

이 외에도 미래인터넷 정보보호 요구사항에 있어서 참고할 수 있는 기능으로는 아래와 같은 다양한 기능들도 함께 고려하여야 할 것이다.

- 이동성에 대한 지원 : 미래인터넷은 이동성/모바일(mobility/wireless)에 대한 지원이 기본적으로 고려되어야 한다. 미래 인터넷은 현재보다 더 단순한 이동성에 대한 해결책과 일정 수준 이상의 성능을 보장해야 한다.
- 유연성과 확장성 : 미래 인터넷은 반드시 다양한 아키텍처가 공존할 수 있도록 설계되어야 한다. 미래 인터넷 아키텍처는 단일하게 홀로 존재하기 힘들기 때문에, 아키텍처가 유연하고 확장 가능하도록 구상되어야 한다.
- 확장성 지원 : 미래인터넷에서는 다양한 응용 프로그램과 서비스들에 효율적으로 대응할 수 있도록 통합된 확장성을 제공하여야 한다.
- 크로스 레이어 기능 지원 : 현재의 인터넷은 레이어링(Layering) 원칙이 정확히 지켜졌으나, 미래 인터넷에서는 크로스 레이어를 지원할 수 있어야 한다. 이는 특히나 정보보호 기능 제공에 있어서 매우 유용할 것으로 보인다.



(그림 4) 상황별, 수준별 정보보호 기능 제공

또 다른 관점에서의 정보보호 요구사항을 한가지 살펴보면 계층적, 수준별 정보보호를 지원하기 위한 네트워크 장비에서의 정보보호 요구사항이 있다. (그림 4)와 같은 일반적인 인터넷 환경에서 사용자의 상황 인지에 따른 적절한 사용자 지원 서비스를 제공하기 위해서는 가상화된 네트워크 환경이 수시로 생성, 소멸될 수 있어야 할 것이다. 이러한 환경에서 상황별, 수준별 정보보호 기능을 제공하기 위해서는 네트워크 내에서 이를 지원할 수 있는 새로운 라우팅 프로토콜이 정의되어야 하며, 네트워크 내의 각종 장비들에서 유효 적절한 동작이 사용자의 상황에 따라 수시로 업데이트 될 수 있어야 한다. 또한, 이러한 네트워크 장비내에서 상호간 교환되는 정보들을 활용하여 악성코드와 같은 네트워크 위협 트래픽에 대한 적절한 방어책을 실행할 수 있을 것이다.

5. 결론 및 향후연구

본 기고문에서는 미래 인터넷이 나타나게 된 원인을 살펴보고, 미래 인터넷에서 나타날 수 있는 보안 위협 및 그 대응방법과 미래 인터넷 정보보호 요구사항에 대해서 기술하였다.

현재까지 이야기되고 있는 미래인터넷이란 현재 인터넷의 문제점과 다양한 미래 요구사항(광대역, 이동성, 안정성, 유비쿼터스성, 경제성, 보안성, 관리성 등)을 수용하는 새로운 미래 네트워크로서, 사용자는 모든 사물과 장치가 네트워크로 연결된 유비쿼터스 컴퓨팅 환경에서 시간과 장소에 관계없이 자신의 상황에 맞는 최적의 서비스를 끊김없이 제공 받을 수 있는 네트워크를 의미한다. 이러한 미래 인터넷에 대한 접근 방식은 현재의 기술을 점진적으로 보완하여 사용하자는 점진적 접근(Evolutionary approach) 방법과 현재의 인터넷과의 호환성을 고려하지 않는 새로운 백지상태(clean slate)에서 시작하자는 근본적이고 혁신적인 접근(Revolutionary approach) 방식이 혼재되어 나타나고 있다.

오늘날의 인터넷에서 가장 중요한 문제의 하나는 보안성(기밀성, 무결성, 가용성 등을 통칭) 문제이다. 이를 통해 현재의 인터넷에서는 악성코드로 인한 네

트워크 안전성 위협, 온라인 사기, 서비스거부공격, 스팸메일과 유해 정보의 범람 등과 같은 역기능 들이 매우 높은 편이다. 이는 효과적인 정보보호에 대한 고려없이 설계된 현재 인터넷의 근원적인 문제에 속할 것이다. 따라서, 미래 인터넷에서는 반드시 이러한 보안 위협에 대해 최우선적인 고려하에 설계되어야 하며, 이를 위한 연구 활동도 활발히 이루어져야 할 것이다.

그러나, 현재의 문제는 잘 알고 있는 반면에 미래 위협에 대응하기 위해 미래 인터넷이 지향해야 할 정보보호 기능은 명확하지 않는 것이 현실이다. 이러한 시점에서 본 기고문에서는 미래 인터넷에서 요구되어지는 정보보호 요구사항에 대해 몇가지 고려사항들을 검토하여 보았으며, 이러한 논의를 기반으로 미래 인터넷에서 나타날 수 있는 정보보호 위협, 이를 해결하기 위한 정보보호 프로토콜, 메커니즘, 기능, 정보보호 요구사항 등에 대해서는 추가적인 연구 활동이 있어야 할 것이다. 특히, 미국, 일본, 유럽과 같은 선진국과의 미래 인터넷 경쟁력 확보 및 시장 창출에 있어 적절한 대응 활동도 필요할 것으로 보인다.

참 고 문 헌

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

[2] 김영화, "미래인터넷의 네트워크 가상화 기술 동향", 전자통신동향분석 제25권 제1호, pp.132~147, 2010. 2월

[3] 변성혁, "미래인터넷 아키텍처 연구동향", 전자통신동향분석 제24권 제3호, pp.1~12, 2009. 6월

[4] 신명기, "미래인터넷 기술 및 표준화 동향", 전자통신동향분석 제22권 제6호, pp.116~128, 2007. 12월

[5] H. Bos, E. Jonsson, E. Djambazova, K. Dimitrov, S. Ioannidis, E. Kirda, and C. Kruegel, "Anticipating Security Threats to a Future Internet", White Paper, http://www.ict-forward.eu/, March 2009

[6] The FORWARD Consortium, "D3.1: White book: Emerging ICT threats", 7th FP, http://www.ict-forward.eu/, January 2010

[7] H. Bos, S. Ioannidis, E. Jonsson, E. Kirda and C. Kruegel, "Future threats to future trust", Proceedings of the Future of Trust in Computing Conference, Berlin, Germany, July 2008

[8] 김성수, 최미정, 홍원기, "미래 인터넷 연구 동향과 관리기능 정의", KNOM 2008, 2008. 4월

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

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

[11] 서동일, 이상호, "1.25 인터넷 침해사고의 분석과 대책", 대한전자공학회지, 제30권 제6호 pp.49~57, 2003.6

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

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

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

[15] EU 7th FP, The Future of the Internet, http://cordis.europa.eu/ict/ch1

[16] EU, "Future Internet 2020", http://www.future-internet.eu, May 2009

[17] Future Internet Forum, http://fif.kr

[18] 안원호, "미래인터넷 정책 추진방향", TTA Journal No.124, pp.30~34, July 2009

◐ 저 자 소 개 ◑

서 동 일

1989년 경북대학교 전자공학과 졸업 (공학사)
1994년 포항공과대학교 정보통신공학과 졸업 (공학석사)
2004년 충북대학교 대학원 전자계산학과 졸업 (이학박사)
1989년~1992년 삼성전자(주) 연구원
2006년~2007년 Department of Computer Science, Purdue University (Visiting Researcher)
1994년~현재 한국전자통신연구원 팀장(책임연구원)
2010년~현재 충남대학교 컴퓨터공학과 겸임교수
2002년~현재 ASTAP-Forum Information Security Expert Group 의장
1994년~현재 TTA 정보보호/네트워크 표준화 전문가 (현재 TC5 부의장)
관심분야 : 인터넷 정보보호, 미래 인터넷, 네트워크, 해킹 기술 등

장 종 수

1984년 경북대학교 전자공학과(공학사)
1986년 경북대학교 전자공학과(공학석사)
2000년 충북대학교 컴퓨터공학과(공학박사)
1989년~현재 한국전자통신연구원 책임연구원
2004년~2008년 한국전자통신연구원 네트워크보안그룹 그룹장
2000년~2003년 한국전자통신연구원 네트워크보안구조팀 팀장
2004년~현재 한국정보보호학회 이사(부회장)
2007년~현재 한국정보처리학회 협동이사
2007년~현재 OSIA(개방형컴퓨터통신연구회) 이사
2006년~현재 대검찰청 디지털수사자문위원회 위원
2006년~2008년 행정안전부 전자정부서비스보안위원회 실무위원
2008년~현재 방송통신위원회 인터넷정보보호협의회 안전인터넷분과 위원
관심분야 : 네트워크보안, 모바일보안, 사물통신망보안 등