情 報 保 護 學 會 誌
第 12 券 第 4 號, 2002. 8

ITU SPU 정보보호 워크샵 보고

류 걸 우*, 손 승 원*, 정 교 일*, 진 병 문**

요 약

본 논문에서는 지난 5월 서울에서 개최된 ITU SPU 워크샵 내용에 대하여 간략하게 기술, 보고하고자 한다. 이러한 회의 내용 검토를 통해 ITU의 보안관련 현재 및 앞으로의 활동 상황에 대해 알아보고, 이를 통해 우리의 활동에 참고가 되고자 한다.

Ⅰ. 서 론

ITU(국제전기통신연합)와 정보통신부 주최로 2002년 5월 20일부터 22일까지 서울에서 "Creating Trust in Critical Network Infrastructure"라는 주제로 Initiative 워크샵이 개최되었다.

이 ITU SPU (Strategy & Policy Unit) 워크샵은 ITU Utsumi 사무총장의 "새로운 시도"라는 프로그램의 한 부분으로 개최되었으며, 목적은 주요 정보통신 기간 시설 보호를 통한 사이버 공간에서의 신뢰 구축을 위한 기술, 경제, 사회적 대응 방안 수립이다. 즉, 워크샵 결과를 토대로 새로운 주제들을 ITU 사무총장에게 권고하고, 정책 결정자, 제도 입안자 및 산업체를 위한 주요 정보통신 기간 시설 보호에 대한 각 국의 현황 조사를 통하여 정보와 의견을 교환하고, 국제적 경험을 공유하도록 함이 이 워크샵의 주요 목적이 되는 것이다.

이 워크샵에는 세계 각국에서 70명의 정책 결정자, 제도 입안자 및 산업체 보안 전문가들이 참가하였으며, 진행은 Harvard 대학의 Deborah Hurley 교수가 의장을 맡았다.

워크샵을 위해 3편의 발제 논문이 발표 및 토의되었으며, 이는 다음과 같다.

- 채기준(이화여자대학교)의 "주요 정보통신 기반 시설에 대한 일반적 개요"
- Seymour Goodman (Georgia Institute of Technology) "주요 정보통신 기반시설에 대한 보안 강화를 위한 국제협력"
- Stephen Bryen (Aurora Defense) "글로벌 주요 기반 시설보호를 위한 종합적 보안 접근"

또, Brazil, Canada, Korea, Netherlands에서 국가 사례 연구를 준비하여 발표 및 토의가 이루어 졌다. 이전에 개최된 ITU-T SG17 워크샵은 주로 기술적인 면에서 이루어지는 반면, SPU 워크샵은 정책 및 관련 규제 그리고 가능한 국제 협력 분야에 대한 것이다.

본 고는 이 워크샵을 통해 발표 및 토의된 내용을 요약한 것으로, 최근 사건에 대한 문제의 본질을 분석하고, 국제 협력의 필요성, 현재 해야 할 일과 앞으로 할 일로 구분하여 정리한 것이다. 마지막으로, ITU-T SG17 의 정보보호워크샵에 대한 내용을 간략하게 기술한다.

Ⅱ. 문제의 본질

전기적 통신 사용과 관련 보안에 대한 논쟁은 새로운 것은 아니다. 그러나, 인터넷이나 정보 통신 네트워크가 우리의 일상 생활에서 중요한 부분이 되어감에 따라 그 기반 시설에 대한 의존성도 또한 중요한 부분이 되었다. 공교롭게도, 우리의 의존성이 증가할수록 기반시설에 대한 적대적 공격 또한 증가하고 있다. 새로운 공격 유형, 공격 도구들과 컴퓨터 소프트웨어의 결함으로 네트워크는 점점 더 취약하게 되었다. 단순 바이러스에 의한 경제적 손실 또

* 한국전자통신연구원 ({kwryu, swsohn, kyoil}@etri.re.kr)
** 한국정보통신 기술협회(bmchin@tta.or.kr)

한 세계적으로 수십억달러에 달한다. 인터넷에 대한 정교한 DdoS(Distributed Denial of Services) 공격 또한 증가하고 있는 실정은 이미 인지하고 있다. 일반적인 정보보호를 위한 대응 방법은 단순히 방어 대책이나 지속적인 소프트웨어 패치와 같은 것들이다. 사실, 이는 공격자 우위의 군비 확장 경쟁과 같은 것으로, 공격자는 이용할 수 있는 취약한 한 부분만이 필요한 반면, 방어자는 모든 가능한 공격에 대해 방어를 하여야 한다. 현실에서 우리는 중요 네트워크 기반 시설의 고장에 따른 이러한 함축적 의미를 제대로 이해하고 있지 못하다.

중요 기반 시설에 대한 정의는 그것이 어디에 사용되어지는 지에 따라 다르다. 따라서 네트워크 기반시설이 공공용인지 혹은 사설용인지, 국가간 대용량의 데이터 전송 능력 등과 같은 것이 확인되어져야 하며, 이는 본 ITU 워크샵의 목적이기도 하다. 중요 네트워크 기반 시설들은 국가 보안과 안전이나 높은 재정적 가치를 가지는 정보를 전달하는 네트워크 이다. 워크샵의 활동 범위는 이러한 기반시설 및 보안, 이용성 및 기반 시설들에 대한 국민적 신뢰도들에 초점이 맞추어져야 한다.

따라서, 본 워크샵의 목적은 가능한 새로운 부분을 찾아 보고하는 것이다. 또 다른 목적은 정책 및 규제와 기술적인 관점에서의 기간망 보호에 관하여 회원국 및 참가자들에게 중립적 토론의 장을 마련하는 것이다. 향후의 목적은 상호 이익을 위해 이 분야에 있어서 정보의 교환을 증진하고, 국제적으로 경험을 공유하는 것이다.

주요 기간 시설 보호란 정보 및 통신 시스템에 대한 기밀성, 보전성, 유용성과 인증을 등을 제공하는 것이다. 글로벌 네트워크를 포함하는 정보 및 통신 시스템들은 동적이며 지속적으로 변한다. 따라서, 주요 기간 시설의 완전하고 전체적인 보호는 불가능하다. 더욱이, 주요 기간 시설 보호란 상대에 대해 배우는 것이다. 그럼에도 불구하고, 유형 자산 보호는 주요 기간시설 보호의 중요한 부분이며, 정보 통신망은 광범위한 문제 중 하나일 뿐이다. 그러므로 주요 기간 시설 보호를 위한 계획을 세울 때 인터넷만 고려하는 것은 부족하며, 대신 어디에나 존재하는 보편한 정보 환경을 고려해야 한다. 정보 및 통신 기술과, 바이오기술 및 나노기술과의 급속한 융합에서와 같이 현재의 정보 및 통신 시스템을 변화시키려는 아주 많은 개발이 진행되고 있다. 인터넷은 함축성, 편재성, 무한성, 분산성, 함축성의 특징들로 나타나는 정보 환경으로 인해 아주 빠르게 성장하고 있다.

여기에서, 주요 기간 시설 보호 관련 대부분의 문제점들은 기술적인 면이 아니다. 그 중 가장 중요한 문제는 크고 복잡한 조직들에 대한 관리이다. 심각한 문제는 freeware와 공개 소프트웨어들을 고려해 볼 때, 제품과 서비스의 bug에 대한 소프트웨어 개발자들의 잠재적인 책임이다. 주요 기간시설 보호, 사이버테러, 그리고 정보 전쟁은 연속체를 형성하고 있다. 이 모두는 주요 기간 시설의 기능의 정상 동작 유지와 연관되어 있다. 따라서 주요 기간 시설보호를 위해 세워진 대책들은 모든 영역에서 참고가 될 수 있다. 각 영역들은 근본적으로 행위자와 그들의 의도에 따라 서로 다르다. 사이버 테러리즘과 정보전쟁이 공공의 많은 관심을 받아왔지만, 주요 기간 시설에 대한 대부분의 위협과 침해는 해커나 크래커 그리고 테러리스트들에 의해서가 아니라 부주의하고, 피로하며, 그리고 제대로 훈련이 되지 않은, 그리고 스스로 인지하지 못한 채 침해와 취약성을 유발시키는 근로자들이다 라는 사실이다.

한편, 인터넷이 사회 전반에 걸쳐 점점 광범위하게 사용되어 대량 전달 매체화되어 감에 따라, 그 성능 기준과 QoS 요구 사항들 또한 빠르게 변하고 있다는 것은 주목할 만하다. 초기의 인터넷 성능 기준은 best effort 이었다. 이러한 QoS의 성능과 보장은 이제 더 이상 충분하지 않으며, 전화 서비스와 긴급 서비스에 적용된 것과 유사한 표준이 - constant availability - 요구되게 되었다는 것이 토의되었다. 표준에 이러한 성능 기준이 결정되어야 하는지, 그리고 이것이 전화나, 긴급 전화서비스, 전기규정 혹은 다른 표준과 유사한지 검토할 가치가 있다. 인간 활동은 주요 기간 시설의 지속적인 작용을 혼란시킨다. 사실 인간 활동은 글로벌 네트워크의 지속적인 정상 동작을 위해 10대들을 포함한 전 세계 인간들의 호의에 점점 더 의존적이다. 많은 정책적 문제들은 사법권, 상호 원조, 증거, 형사 소추 등과 같은 것들로부터 발생된다. 또, 보안 이슈에 대해 조직적이고 계속적이며, 그리고 사용자에 대한 교육 및 훈련을 활성화시키는 접근의 필요성에 대한 의식을 확산시키는 것은 중요하다. 10대들이 해커화되는 것을 억제하고 보안 문제에 대한 이해를 증진하기 위해서, 학생들을 포함한 모든 수준의 교육 및 훈련 프로그램들이 개발되어야 한다.

주요 기간 시설 보호는 일상의 기업활동과 사생활

에 대한 확실한 동작이라는 것 뿐만 아니라 불가피하게 야기시키는 법의 집행과 국가 보안에 대한 사항들을 포함한다. 이것은 또한 전기, 에너지, 수도등과 같이 다른 중요한 자원에 대해서도 사실이다. 법 집행과 국가 안보에 대한 문제점들은 충분히 고려되어져야 하는 반면, 그것들은 시민 사회에서의 이러한 주요 기간 시설의 사용 관점에서 성취되어야 한다. 주요 기반시설 보호에 대한 위험 감내, 평가, 그리고 관리에 대해 더 많은 연구와 이해도 향상이 필요하다. 이러한 관점에서 볼 때, 위험에 대해 유익한 교훈을 주요 기간 시설 보호라는 영역에 적용하기 위해 보험 산업과 같은 유사한 분야를 연구하는 것도 매우 유용할 것이다.

그리고, 컴퓨터 보안에 대해서는 아주 많이 알려져 있으나, 보안 대책 적용의 계속적인 실패와 함께 그 실현은 아주 뒤떨어져 있다. 이러한 결함에는 여러 이유가 있다. 보안 취약성, 위협 및 침해에 대한 자료가 부족하다. 사설 부분에 있어서 주요 기간 시설 보호를 향상시키도록 촉진시키는 보장 구조가 없다. 더 좋은 자료는 향상된 기간 시설 보호를 잘 나타낼 수 있기 때문에 유용하다. 이것은 보험 요구, 책임/의무, 표준, 그리고 연구개발 및 세금공제 등과 같은 보장 구조의 설치를 통해 실현되어져야 한다.

글로벌 네트워크의 본질적인 보안은 항상 나빠지고 있다. 이러한 증가하는 위험에 영향을 미치는 요인들로는 컴퓨터, 통신망, 자료, 정보, 그리고 오류를 범하기 쉬운 사람들의 지속적인 증가이다. 더불어, WWW에 대한 해킹 도구의 유용성과 해커의 필요한 전문성은 반비례한다. 주 관심은 기업이나, 개인, 그리고 정부 조직들이 보안 대책을 세우도록 그들을 장려하는 방법이다. 참석자들은 세금 감면 등과 같이 보안 수준을 향상 시킬려는 의도를 높이도록 하는 보장 구조의 필요성을 지적하였으며, 보안 문제는 근본적으로는 기술적인 것이 아니라는 것에 동의하였다. 위협에 대한 안전한 프로토콜과 기술적 해결책은 존재한다. 그러나, 그것들을 실행할 정치 경제적 의지가 때때로 부족한 것이다.

Ⅲ. 국제 협력의 필요성

워크샵 기간동안 발표와 토의에서 반복되는 주제는 주요 정보 통신망 기간 시설 보호를 위한 국제적인 협력이 필요하다는 것이었다. 현재 수준의 협력은 여러 관점에서 부족하다는 것에 동의하고 있다. 더욱이, 거의 모든 국가에 있어서 국가의 활동이 부족하고 조직적이지 못하다. 기간 시설 보호에 대한 개선된 주의와 활동이 국제적 그리고 국가적 모든 단계에서 필요하다. 증진된 국제적 노력과 협력은 국가 업무를 수행함에 있어서 중요하고 효과적인 자원을 제공한다. 국제적 협의는 합의를 도출하고 접근 방법에서 일치성을 제공하는데 도움이 된다. 이것은 예측 가능성, 응집성, 지속성, 확실성에 있어서 글로벌 네트워크를 보호하는데 중요하다.

국가간 그리고 영역간 협조는 현재 제한되어 있으며, 그것은 종종 개인적인 관계에 의존하고 있다. 다양한 수준의 협력은 여러 국가법에 의해 제약을 받으며, 그러한 정보의 상호 교환에 그러한 제약이 적용되고 있다. 개인적인 관계에 의해서가 아닌 절차에 기반을 둔 협력 방법이 정립될 필요가 있다. 주요 정보통신 기간시설 보호와 관련된 에이전트들이 공격이나 위협에 대해 다른 국가의 에이전트들과 적극적 협력이 가능하도록 위임권을 가질 필요가 있으며, 협력 증진을 위하여, 법과 지침 혹은 정책들은 국제적인 수준의 간결 명료하여야 한다.

Ⅳ. 현재 해야 할 작업

일단 광범위한 국제적 협력이 확실히 필요하다는 것이 결정되면, 협력 형태에 대해 고려하여야 한다. 한 예로, Goodman 교수는 그의 논문에서 국제 협력에 대한 5가지 프레임워크를 제시하였다.

- 국제 표준 : 표준 개발에 있어서 국제 협력의 중요성이 증가하고 있으며, 이는 경쟁 시장에서 조차도 마찬가지다. 또한 표준 설정과 구현에서의 협력도 중요하다.
- 정보 공유 : 약점 노출과 공공의 신뢰 손상에 대한 두려움 때문이라면 사이버 공격에 대한 정보 공유 거부가 가능하다. 믿을만한 정보 저장소처럼, 국제적 조직이 담당해야 하는 어음교환소 기능과 같은 역할이 있을 수 있다. 그러한 어음교환소는 정보수집과 유포를 조정하는 것뿐만 아니라 피해에 대해 익명성을 제공해야 한다.
- 진행중인 사이버 공격 중지 : 특히 사이버 공격이 진행되고 시간이 본질인 경우 국경을 통한 정보 교환에 대한 표준화 방법을 개발하는 것이다. Dr. Bryen은 사이버경보센터의 설립을 제안하였으며, 이는 공통 자료의 보고 표준을 설

정하고, 경보 서비스처럼 동작한다.
- 법률 시스템의 조화 : 범죄와 테러 활동에 대한 방어를 할 때, 해커들이 안전한 지역을 찾지 못하도록 법률 장치들에 대한 협력이 있어야 한다.
- 개발국가에 대한 원조 및 지원 : 이것은 ITU 회원국들간 경제적 기술 개발의 다양한 수준의 협력을 필요로 한다.

국제협력 프레임워크를 개발하는 데 있어서, 공식/비공식, 다원적/이원적, 능동적/수동적 등 3차원의 협력을 고려하는 것이 유용할 것이다. 아울러, 성공적인 국제 협력은 국가와 자치 단체 수준의 효과적인 협력에서 먼저 나타나야 한다. 국가사례 및 발표에서 이러한 분야의 여러 문제점들을 나타내었다.

V. 이후의 작업

정부는 적절한 활동 계획을 세우기 위해 취약성과 국가 네트워크 위험에 대한 위험 평가를 수행하고 있다. 현존하는 적절한 방법, 활동, 그리고 이미 주요 기간시설 보호에 적용중인 규정 등을 확인하는 것이 유용하다고 하였다. 추가적으로, 현존의 적절한 방법 및 활동과 기간 시설보호에 대한 이슈들의 영향에 대해서 이미 활동하고 있는 단체들을 확인하는 것도 유용할 것이라 토의하였다.

인터넷을 포함한 발전된 정보 통신망들은 주요 통신 기간 시설에 매우 의존적이다. 이와 유사하게도, 인터넷 서비스들은 공공의 전화 서비스를 대신하게 될 것이다. 요약하면, 안전한 망을 제공하고 운영하는데 있어서 전화와 인터넷 서비스 제공자들 모두의 공동 관심은 분명히 있다. 국가 정책과 단속 자세에 대한 검토가 적절할지도 모른다. 하지만 조화를 이루지 못한 정책이나 법규는 정보 시스템의 보안과 네트워크 기간시설 보호에 잠재적으로 그 발전을 저해한다.

기간 시설 보호에 대한 문제가 다차원적이기 때문에, 하나의 국제적 포럼이 정보시스템 보안과 네트워크 기간시설 보호를 해결할 수 있을지도 모른다는 사실이 고려되어졌다. 따라서, 여러 국제적 토론회에서 특정 분야를 발전시키는 방향으로 작업하는 것이 가장 이로울 것이다. 공공의 혹은 사설 영역 기반에 관계없이 적절한 포럼은 정부 조직인지 혹은 비정부 조직인지 확인되어야 한다.

이와 함께, ITU의 역할과 관련하여, 다음의 제안에 대해 토의하였다.

- ITU는 조속한 시일 내에 현재의 work program 활동을 정보 시스템의 보안과 네트워크 기간시설 보호와 비교하여 검토하여야 하고, 이러한 분야에서 그 활동을 강화할 행동을 취해야 한다. ITU는 이러한 분야에서 차별화된 국제적 포럼으로 대표될 수 있다.
- 정보 및 시스템 보안에 대한 개선된 기술적 표준의 필요성, IP 관련 취약성에 대한 개선된 협력, 그리고 ITU와 다른 표준 단체들간의 개선된 보안 표준들의 필요성이 언급되었다.
- ASN.1 구현 관련 가능한 취약성을 조사하기 위한 전문가들과 ITU-T와의 협력에 대한 언급이 있었다.
- 정보시스템의 보안과 네트워크 기간시설 보호라는 주제는 WSIS (World Summit for the Information Society)의 의제에 포함되도록 제안되었다.
- 본 워크샵에서 시작된 토의가 앞으로 계속되도록, ITU 웹 사이트에 게시판을 설치하도록 제안되었다.
- 국가나 지역적인 보안 증명 표준이 존재하고 있지만, 보안 증명의 국제적 상호 인정 방법 개발을 고려하여야 한다.

VI. ITU-T SG17 정보보호 워크샵

ITU-T의 워크샵은 ITU-T내의 정보보호 표준화 연구 관련 선도 그룹(Lead SG)인 SG17 (Data Network and Telecommunication Software)이 중심이 되어, 그 동안 ITU-T 산하 여러 연구반(SG)에서 산발적으로 추진하고 있는 정보보호 관련 표준화 연구를 집중 통합 관리하고, 향후 보다 강화된 협력 체제를 구축하기 위하여 개최되었다. 2001년 인도 회의에서 SPU 워크샵과 함께 한국 개최를 유치하한 것으로, 20여개국으로 부터 정보보호기술 전문가 200여 명이 참석하였으며, 총 20여 편의 논문이 발표되었다.

이 워크샵의 목적은

- 통신망 기반 정보보호 관련 기술 및 표준화 이슈의 공개적 논의
- 정보보호에 대한 인식제고 및 대응책 마련

- ITU-T 정보보호 관련 표준화 이슈의 재정리 및 통합관리
- 국제표준화 기구와의 정보보호 관련 표준화 연구 협력 등이다.

이 워크샵에서 발표된 자료는 ITU 홈페이지에 게재되어 있어, 별도의 설명은 약한다.

그리고, 워크샵 마무리를 위한 패널 토의에서는 다양한 의견이 제시되었는 데, 가장 큰 이슈로 정보보호 분야에서의 ITU-T 역할에 대한 토의에 많은 시간을 할애하였다. 특히, 지역적 정보보호 문제 토의시 세계 최고의 인터넷 인프라를 구축한 한국의 경우 전자 문서 교환 및 전자상거래의 안전 . 신뢰성을 보장하기 위한 전자서명 서비스가 강화될 필요가 있으며, 또한 최근의 스팸메일에 대한 문제점을 지적하고, 현재 정부가 정책적으로 이에 대처하고 있음을 보고하였다.

Ⅶ. 맺음 말

지금까지 지난 5월에 연속으로 개최된 ITU 워크샵에 대한 내용을 간단하게 정리하였다. 먼저 개최된 SG17 워크샵은 주로 기술적인 면을, 다음 주에 개최된 SPU 워크샵은 정책적인 면을 많이 다루었다. 본 고에서는 기술적인 토의는 자료를 확보하여 독자가 쉽게 이해할 수 있다고 보고, 주로 SPU 워크샵의 내용을 중심으로 정리하였다.

한국의 정보보호 표준화 활동은 주로 IETF, ISO/IEC JTC1 등에서 많이 이루어지고 있으나, 이번 2개의 워크샵을 계기로 정부간의 표준화 기구인 ITU-T에 대해서도 많은 상향식 표준화 활동과 정책적인 대응이 있어야 할 것으로 판단된다. 향후 초고속 정보통신망에서의 정보보호에 대한 사회적 수요가 높기 때문에 정보보호 표준 개발 및 제정이 더욱 활발해져야 하며, 이를 바탕으로 관련 국내 산·학·연·관이 협력하여 동 분야의 기술력 강화 및 정책적 지원은 물론 국제표준화 활동도 한층 더 강화되어야 할 것으로 사료된다.

참고문헌

[1] http://www.itu.int
[2] TTA, TTA 저널, 제81호, 2002. 6.

〈著者紹介〉

류 걸 우 (Gul-Woo Yu)
1990년 5월 : MS. Computer Science, Unv. of Massachusetts, MA, USA,
1993년 5월 : ScD. Computer Science, Unv. of Massachusetts, MA, USA,
1994년 7월~현재 : 한국전자통신연구원, 정보보호연구본부 / 책임연구원,

손 승 원 (Sung-Won Sohn)
정회원
1984년 : 경북대학교 전자학과(공학사)
1994년 : 연세대학교 산업대학원 컴퓨터공학과(공학석사)
1999년 : 충북대학교 대학원 컴퓨터공학과 (공학박사)
1991년~현재 : 한국전자통신연구원 정보보호연구본부 네트워크보안연구부장 / 책임연구원
관심분야 : 이동인터넷보안, 네트워크 보안

정 교 일 (Kyo-il Chung)
정회원
1981년 : 한양대학교 전자공학과 (공학사)
1983년 : 한양대학교 산업대학원 전자계산학과 (공학석사)
1997년 : 한양대학교 대학원 전자공학과 (공학박사)
1982년~현재 : 한국전자통신연구원 정보보호연구본부 정보보호기반연구부장 / 책임연구원
관심분야 : IC Card, Security, Biometrics, 국가기반보호, 신호처리

진 병 문 (Byoung-Mun Chin)
1976년 2월 : 서울대학교 전기공학과 학사
1983년 8월 : 서울대학교 대학원 전자계산공학과 석사
1996년 2월 : KAIST 전자계산학 박사
1980년 4월~2001년 4월 : 한국전자통신연구원 근무
2001년 4월~현재 : 한국정보통신기술협회 표준기획본부 본부장