미국의 정보인프라 보호 연구개발 동향 분석

A Study on the Research and Development Trend for Information Infrastructure Protection in U.S.A.

전용희(Y.H. Jeon) 보안게이트웨이연구팀 초빙연구원, 대구가톨릭대학교 컴퓨터정보통신공학부 교수
장종수(J.S. Jang) 네트워크보안그룹 책임연구원, 그룹장
손승원(S.W. Sohn) 정보보호연구단 책임연구원, 단장

2003년 1월 25일 '인터넷대란'이 발생한 이후 특히 정보인프라 보호에 대한 관심이 증대되어, 국내에서도 정보인프라 보호를 위한 정보보호 기술 개발에 대하여 많은 연구 활동이 진행되고 있다. 그러나 아직도 해결해야 할 문제점들이 많이 남아 있다. 그 동안 정보보호 제품, 기술 개발 및 연구동향을 소개하는 문헌은 있으나, 정보인프라 보호에 대한 연구개발 동향을 폭 넓게 소개하는 문헌이 없고, 더구나 연구개발 분야에 대하여 보다 자세한 내용 기술이 필요하다고 사료된다. 본 고에서는 정보보호 수준이나 대응체계가 훨씬 앞서 있는 미국의 정보인프라에 대한 연구개발 동향을 분석 기술함으로써, 향후 국내의 정보인프라 보호 연구개발 방향 정립에 이용하고자 한다.

I. 서 론

미국 정부는 2002년 7월 각종 위협으로부터 본토의 안전과 자국민의 보호를 위한 목적으로 'Homeland Security' 계획을 발표한 바 있다[1]. 또한 같은 해 9월 안전한 사이버 공간을 위한 국가 전략(National Strategy to Secure Cyberspace)을 발표했는데, 사이버 보안을 위해 인식(awareness)과 정보, 기술과 도구, 훈련과 교육, 역할과 제휴, 연방정부 지도력, 조정과 위기관리의 6가지 도구를 제시하였다.

사이버 보안을 위한 국가 전략은 9.11 테러 발생 후 시행되었는데, 새로운 조직인 국토안보부를 연방정부 안에 신설하고, 미국을 위협하는 모든 위험요소에 대해 국가의 안전과 본토 자국민에 대한 보호를 강화하고, 생화학이나 핵무기 등에 의한 공격 등 물리적인 위협뿐만 아니라 사이버위협에 대한 대비를 강구한 의의가 있다[2].

국내에서도 2003년 1월 25일 '인터넷대란'이 발생한 이후 정보인프라 보호(Information Infrastructure Protection: I2P)에 대한 관심이 증대되었다. 그 결과의 일부로 2004년 3월 18일 세계적인 보안업계인 시만텍의 '인터넷 보안 위협 보고서'에 의하면 국제적인 해킹에 우리나라의 시스템이 악용되는 해킹 근원지 조사 결과, 2002년 하반기 2위에서 2003년 하반기에는 7위로 많이 낮아져, 국내의 보안 인프라와 일반 사용자의 보안 의식이 크게 개선된 것을 보여주고 있다[3].

그러나 아직도 해결해야 할 문제점들이 많이 남아 있다. 국내에 정보보호 제품, 기술 개발 및 연구동향을 소개하는 문헌들이 존재하나, 정보인프라 보호에 대한 연구개발 동향을 폭넓게 소개하는 문헌은 아직 존재하지 않고, 더구나 연구개발 분야에 대하여 보다 자세한 내용 기술이 필요하다고 사료된다[4]-[9]. 이에 따라 본 고에서는 정보보호 수준이나 대응체계가 훨씬 앞서 있는 미국의 정보인프라에 대한 연구 개발 분야를 고찰함으로써 향후 국내의 정보인프라 보호 연구 개발 방향 정립에 기여하고자 한다. 본 고에서는 미국의 I3P(The Institute for Information Infrastructure Protection)의 보고서 내용을 중심으로 미국의 정보인프라 연구개발 동향에 대하여 기술하고자 한다[10],[11].

II. 연구주제 및 기능별 영역 동향

I3P는 사이버 보안과 정보인프라 보호 연구개발에 초점을 맞춘 23개의 학교 및 비영리 연구조직의 컨소시엄으로 구성되어 있으며, 본 절에서는 미국 내의 사설 부문 및 정부 지원 연구 활동의 집합체에 의한 정보인프라의 보안에 대한 중요한 가치가 있는 토픽들을 식별한다. 그 대상은 2002년도에 수집되고 분석된 정보에 기반하고 있으며, 산업체, 정부 및 학교 전문가의 입력을 반영하고 있다. 연구 활동의 포함 기준은 대표성 혹은 중요성이다.

I2P 관련 연구에서 광범위한 주제는 다음과 같다[11].

- 생존성(survivability)
- 평가력(assessability)
- 구성력(composability)
- 자동, 실시간 대응
- 자기-강화 시스템

조사에서 발견된 연구 활동의 수준에 따라 순위를 매긴 보안 기능별 영역의 동향은 아래와 같다[11].

- 암호술(cryptography): 암호술 연구의 가장 강한 두 분야는 아래와 같다.
  - 대표적인 PKI(Public Key Infrastructure) 애플리케이션에서 암호화를 하위계층 네트워크 장치로 임베드하는 쪽으로 암호기술의 확장
  - 양자 레벨 암호술 연구의 증가
- 침입탐지: 침입탐지의 도메인이 경계에서의 차단 및 탐지뿐만 아니라 다음을 포함하도록 빠르게 확장되고 있다.
  - 침입 이벤트에 대하여 시스템을 준비할 수 있는 예측 기술
  - 탐지를 위한 개선된 센서
  - 복구 및 재구성을 포함한 실시간 시스템 대응 능력
  - 침입을 기원까지 역추적하는 능력, 확장된 포렌식(forensics) 능력
- 안전한 배치(구성) 및 시스템 보증: 시스템에게 보안 상태를 동적으로 평가하고 변경하기 위하여 자신의 보안 배치와 능력에 대한 지식을 부여하기 위하여 연구 초점이 맞추어졌다. 이 분야는 진보된 침입탐지 기술과 밀접한 관련이 있다.
- 시스템 백업, 복구 및 재구성: 공격에 대하여 자동적으로 대응하기 위하여 시스템으로 하여금 영향을 받은 시스템을 밀봉하고, 남은 기능을 복구하고, 회복 모드에서 안전한 상태를 재구성하도록 한다.
- 식별 및 인증: 생체인식 및 다른 비전통적인 식별 기술에 초점을 둔 연구가 계속되고 있다.
- 부인 방지 및 인증성: 이 연구분야는 주 연구주제는 아니지만, 진보된 부인방지와 인증성 기술이 시스템 자기-인식과 자기-평가에서 요소로 나타나고 있다. 디지털 저작권 관리(Digital Rights Management: DRM) 영역에서의 관심이 이 영역에서의 연구를 주도하고 있다.
- 무결성 보호: 이동 코드 취급과 적대적 코드 탐지가 약간의 연구 관심을 받았다.
- 경계 보호: 침입탐지에 대한 진보된 방출력(releasability) 기술과 공헌을 포함하여 이 영역에 대하여 약간의 연구 활동이 있었다.
- 권한검증(authorization) 및 접근 통제: 복잡한 분산 시스템의 트러스트 관리에서의 상당한 연구가 권한검증 및 접근통제 상태를 진보시켰다. 또한 이 분야의 연구는 진보된 암호 기술, 비정상 탐지, 불일치 상태와 경고의 자동적인 상호관련에 초점을 두고 있다.
- 감사: 이 영역은 주요한 연구 초점으로 거의 활동이 없었다.
- 보안 행정(administration): 비활성화된 연구영역이다.

III. 영역별 연구 현황

I3P 보고서에서 밝혀진 연구영역은 8개 분야이다. 아래에서 각 영역별로 기술한다[11].

1. 전사적(혹은 통합) 보안 관리

가. 기존 연구

ESM(Enterprise Security Management) 부문의 연구는 일반적으로 다음과 같은 특정 문제 영역에 초점을 맞추고 있다.

- 구성 관리(configuration management): 자동 구성 점검 및 기술된 보안 정책에 일치하는 자동 구성 생성에 대한 노력에 초점이 증가되고 있다.
- 사용자 활동 모니터링: 특권 사용자뿐만 아니라 내부자 모니터링에 대한 연구 관심이 증대하고 있다. 보안 정책 정의와 링크 모니터링 활동에 대한 연구가 필요하다.
- 보안 패치 관리: 사용 시스템에 대한 보안 패치의 영향을 결정하기 위한 방법에 대한 부가적인 연구가 필요하다.
- 이기종 환경에서 보안관리 방법 연구: 역할 기반 접근 제어(Role-Based Access Control: RBAC)와 접근 제어 속성의 모델링 및 사상(mapping)에 대한 연구를 포함한다.

나. 연구 영역

다음은 정보인프라 보호의 상태를 개선하는 데 높은 상승효과를 가질 수 있는 연구 분야이다.

• 통합 정책 정의 및 관리

통합 정책을 정의하고 관리하는 문제는 두 가지 측면을 가진다. 첫째는 통합 목표와 일치하고 실제로 번역 가능한 정책을 어떻게 정의하는가이고, 둘째는 어떤 정책이 통합 시스템에 의하여 실제로 시행될지 어떻게 보안 관리자가 더욱 쉽고 효과적으로 결정하는가이다.

제어의 범위, 입상성(granularity), 보호 강도와 구성의 용이성 모두가 기술 간 일관성 있는 정책 시행에 영향을 준다. 모든 컴포넌트의 실시간 재고(inventory)를 생성하기 위한 도구도 필요하다. 보안 관리자와 사용자 모두에게 더욱 접근 가능한 인터페이스가 필요하며, 무선 네트워크 및 동적 시스템에 확장된, 사용자-친근 그래픽 디스플레이와 같은 시각화 기술이 특별히 필요하다. 통합 보안 관리 결정의 자동화에 대한 연구도 필요하다.

인프라 컴포넌트 사이의 권한검증과 접근 제어의 정의 및 사용자 접근 관리에 대한 특별한 필요성도 있다. 이기종 환경에서, ESM 기술, 데이터 및 데이터 교환의 보안을 보증하는 문제, 다른 형태의 내부자를 고려하여 신뢰된 내부자(trusted insider)의 개념 조사에 대한 연구도 반드시 필요하다. 연구는 도메인 간 접근, 감사(auditing), 감시(monitoring), 증거 수집 및 조사 문제가 어떻게 취급되고, 이런 문제를 다루기 위한 다른 전략의 비밀성 의미를 반드시 고려하여야 한다. 마지막으로, 이런 문제들의 기술적인 면 뿐만 아니라 사회적, 조직적인 면도 연구되어야 한다.

• 목표 위험 형국(posture)의 정의 및 유지보수

기업 환경의 기술적, 비기술적 양면 모두를 고려한 위험 형국을 평가하기 위한 적절하고 유용한 그리고 효과적인 방법론을 개발하기 위한 연구가 필요하다. 새로운 능력은 위험 형국을 폭 넓은 다양한 환경을 위한 구체적인 절차적, 구조적, 기술적인 요구사항으로 변형할 수 있어야 하며, 이러한 환경이 시간에 따라 바뀌는 경우에도 가능해야 한다. 더욱이, 현재 기업 위험 형국이 결정될 수 있거나 혹은 정의된 위험 관리 전략 준수가 평가될 수 있도록 실시간으로 "구축된(as-built)" 환경을 평가하기 위한 능력에 대한 연구가 필요하다.

• 보안 경계 정의 및 보호

보안 경계(security perimeter)는 하나의 보안 정책이 실행될 수 있고, 그 밖에서는 보안 정책과 실행 메커니즘이 단지 가정될 수 있는 경계선을 나타낸다. 경계는 IP 계층뿐만 아니라 모든 계층에서 정의되어야 한다. 그러므로 전사적 보호를 위한 새로운 모델에 대한 연구가 필요하다. 구체적인 문제로는 내부 시스템이 외부적으로 접근 가능할 때 침입에 대한 보호와 손상을 제한하는 방법, 구조적 대안

을 정의하는 방법과 심층 방어 전략이 있다.

2. 분산 자율 파티 사이의 신뢰

정보 인프라는 조직, 시스템, 개인, 이동 전화에서 데스크톱 컴퓨터에 이르기까지 다양한 장비 사이의 상호작용에 의존한다. 어떤 상호작용이 허용되는가에 대하여 파티가 내리는 결정은 트러스트 관계를 토대로 한다. 정보인프라의 성질과 사용이 발전함에 따라, 신뢰 관계의 정의, 확립과 실행도 마찬가지로 수행되어야 한다.

가. 기존 연구

신뢰 관계는 식별(identification)과 기대(expectation)를 포함하기 때문에 많은 연구가 동종 및 이기종 시스템 구조에서 분산 파티의 식별과 인증에 초점을 맞추어 왔다. 동종 환경에서, 기대는 내부 정책 정의와 보안 행정 능력에 의하여 정의되고 관리된다. 현재의 솔루션들은 중앙 기관이나 사전에 결정된 신뢰된 제 3자(보안 관련 정보나 서비스를 제공하기 위하여 신뢰할 수 있는 조직이나 정보인프라 컴포넌트)에 의존한다. 공개키 인프라(PKI)를 통하여 한 행정 경계에서 이기종 컴포넌트에 대한 식별과 인증이 확장된다. 인증기관(CA)인 제 3자가 거래에서의 모든 참가자들을 인증한다. 확장성, 기업 내의 일관된 구현과 관리, 통합 및 사용의 용이성을 포함하여 기존 솔루션과 관계되는 문제를 다루기 위한 연구가 계속되고 있다. 특정 인증 메커니즘과 데이터 접근, 자원 사용, 거래 참가를 위한 권한검증에 대하여 초점을 맞추어 연구가 수행되고 있다.

기존 솔루션을 벗어나, 현재 연구는 피어 대 피어(P2P) 신뢰 모델, 동적 신뢰 확립, 자율 파티 사이의 신뢰 취소, 그리고 신뢰 상대의 부재시 데이터 검증 및 신뢰를 포함하고 있다.

나. 연구 영역

이 연구 영역은 다양한 자율 파티 사이의 모든 측면의 신뢰에 관계된다. 신원확인(혹은 식별), 인증, 보안 관리 도메인에 걸친 활동의 권한검증, 동적 협상, 실행, 보안 관련 협정의 시행 시연, 다른 파티에게 중요한 보안과 기능적 목표 사이의 상호보완(trade-off)(즉, 비밀성 대 편의성), 인프라에서 참가 요소 간 역할과 책임의 정의 및 관리, 증가하는 동적 정보인프라에서 신뢰 관계성의 정의 및 취소 등이 있다.

다음은 정보인프라 보호의 상태를 개선하는 데 높은 상승효과를 가질 수 있는 연구 분야이다.

• 분산 자율 파티를 위한 신뢰모델

이전에 결정된 신뢰된 제 3자가 없는 가운데 신뢰를 확립하고 유지하는 문제는 개념적, 기술적, 사회적 도전 과제이다. 개념적 도전은 주어진 환경에서 파티 사이의 신뢰를 위한 적절한 기초를 결정하고, 관심 있는 행위를 식별하고, 신뢰를 확립하기 위하여 중요한 파티의 속성을 상술하는 것을 포함한다. 다른 문제로 불신(mistrust)이 가정되어야 하는 정도와 주어진 신뢰 모델의 한계 등이 있다.

기술적인 도전은 정책을 구체화하는 새로운 프로토콜 정의, 허용되는 행위에 대한 협정이 자동적으로 협상되고 실행될 수 있는 방법과 메커니즘 식별, 그들의 시연된 실행, 협정에서 동적 변경 관리 기술 식별, 신뢰 상속(inheritance) 혹은 대표(delegation) 관리, 신뢰 취소 관리를 포함한다.

정보인프라에서 신뢰를 증가시키기 위하여 연구가 필요한 사회적 문제점으로는 신뢰 관계 자동 협상 의미의 탐구와 다른 접근방법이 어떤 환경에서 개인과 전사적 사용자에게 수용 가능한가 등이 있다. 사회 과학에서 신뢰 모델의 응용, 채택, 확장에 대한 연구가 필요하다. 이것은 신뢰가 확립되고 유지되는 방법, 누가 누구를 왜 신뢰하는가, 신뢰 수준 혹은 뉘앙스에 관한 것이다.

• P2P 설정에서 동적 보안 관계

위에서 기술된 일반 신뢰모델을 다루기 위한 필요는 계산, 네트워킹, 정보 공유와 같은 P2P 설정에서 특별히 심각하다. P2P 관계는 그들이 참가하는 컴퓨팅 플랫폼 혹은 이동 장치의 취약성을 증가시킨

다. 구체적인 문제로는 신뢰 협상을 위한 하부의 공통분모를 정의하고, 많은 파티들이 옳은 수준의 신뢰에 도달할 수 있도록 하는 안정된 통합 프로토콜을 정의하는 것이다.

• 동적 신뢰 관계에서 파티로서의 장비

점차적으로 장치들이 정보인프라와 동적으로 인터페이스를 가지고, 상호작용하고, 그리고 연결해지된다. 장치들의 형태도 이동 전화, PDA(Personal Digital Assistant), 랩 톱과 같은 전사적 자원, 센서와 프로세스 관리 장치와 같은 특수 목적 장치처럼 점점 더 다양화되고 있다. 위에서 기술된 일반 신뢰 모델 문제들이 인프라 컴포넌트와 그러한 컴포넌트와 일시적으로 상호 작용하는 것과 같이 더욱 특정한 장비 관점에서 다루어져야 한다.

• 데이터에서 신뢰 확립

점점 더 분산된 피어-지향 환경에서 개별 파티(컴포넌트, 사용자, 소프트웨어)에서 데이터 자체로 신뢰를 이동할 필요가 증가하고 있다. 증명-수반(proof-carrying) 코드와 같은 소프트웨어-지향 기술이 데이터에 확장될 수 있는가의 중요한 의문은 어떤 조건에서, 어떻게 정확성과 제시된 데이터의 집합에서 악의가 없음이 소스를 위한 확립된 보안 문맥 없이 평가될 수 있는가이다. 통신 경로 독립성을 제공하는 기술에 대한 연구가 필요하다. 그리하여 데이터는 어떻게 그것이 도착되었는가 문맥이 없어도 무결성과 신뢰 수준을 유지할 수 있다.

3. 보안 성질과 취약성 발견 및 분석

현재 개발중이거나 개발된 시스템들은 취약성과 열악한 보안 성질을 가지고 있다. 정보인프라는 운영 및 재정비용을 초래하는 공격의 지속적인 공세를 받는다. 생명 주기의 모든 단계에서 이용 가능한 결점이 도입되었는지 혹은 예측하지 못한 보안 성질이 도입되거나 상승되었는지를 결정하기 위하여 새로운 방법이나 연구가 필요하다. 가장 시급하게 필요한 것은 소프트웨어의 이용 가능한 취약성을 식별하기 위하여 소스 코드, 목적 코드와 통합 시스템을 분석하기 위한 방법론과 도구이다.

가. 기존 연구

요구되는 보안 성질의 존재를 보증하고 취약성을 예방하는 문제에 대하여 상당한 연구 노력이 경주되어 왔다. 더 정확하게 말하면, 하드웨어와 소프트웨어 구현이 진술된 기대치에 일치하는지를 보증하기 위하여 형식적 방법에 대한 연구가 오랫동안 활발한 연구 분야이었다. 그러나 그 방법은 적용성이 제한되어 대형 시스템이나 시스템들의 시스템을 위하여 실제적임이 증명되지 않고 있다. 현재 연구는 요구되거나 수용할 수 없는 행위의 사양으로부터 테스트 스위트를 자동으로 생성하고 암호 프로토콜 사양의 보안 성질을 분석하기 위한 기술을 포함하고 있다.

많은 취약성이 코딩 오류로부터 초래되는데, 코드 내의 취약성을 방지하거나 가능성을 감소시키기 위한 연구로 안전한 프로그래밍 언어의 개발과 사양으로부터 코드의 자동 생산에 대하여 이루어지고 있다.

악성 코드를 식별하고 분석하기 위한 방법론과 도구를 개발하기 위한 연구도 진행중이다. 바이러스 탐지 제품이 코드 내의 특정 시그너처를 탐지하지만, 다형태 악성 코드 탐지와 소스 혹은 목적 코드 내의 취약성 식별과 같은 더 일반적인 문제들에 대하여는 초보적인 연구단계에 있다. 소스 코드 분석에 대한 현재 연구는 패턴 매칭 탐구, 특징 추출 및 코드 슬라이싱 분석 기술을 포함하고 있고, 목적 코드에 대하여는 비교 분석과 분해(disassembly)-기반 기술이 연구되고 있다. 약간의 진전이 있지만, 대규모 코드를 조사하기 위하여 요구되는 완전성과 품질(예를 들어, 견고성, 확장성)을 가진 능력이 없다.

나. 연구 영역

• 코드 스캐닝 도구와 기술

코드 내의 취약성을 식별하기 위한 능력에 대한 연구가 시급하고 중요하게 요구된다. 이것은 두 개의 하부 범주로 세분된다.

- 소스 코드-스캐닝 도구: 소스 코드를 스캔하고 잠재적인 취약성을 식별할 수 있는 도구가 필요하다. 이 도구는 또한 확장성을 보유하고 사용이 용이해야 한다.
- 목적 코드-스캐닝 도구: 목적 코드에 대하여도 이와 비슷하게 필요하다.

• 장치-스캐닝 도구

하드웨어, 펌웨어, 통신 매체 및 저장 매체와 같은 정보인프라 컴포넌트의 다른 요소의 자동 분석에 대한 연구도 필요하다.

• 발견 및 분석 방법론

특정 코드와 장치-스캐닝 기술 및 구현 이외에, 보안 성질의 발견 및 분석을 위한 광범위한 방법론이 필요하다. 좀 더 일반적 방법론이 필요한 특정 분야의 예로, 제어 및 구성 세팅의 발견 및 분석, 프로토콜 분석, 시스템 보안 성질의 발견, 시스템의 행위 스캐닝이 있다.

4. 신뢰 시스템과 네트워크 대응 및 복구

지금까지의 보안 분야의 연구 개발은 탐지에 초점을 둔 정보보호에 대한 것이 주류를 이루었다. 복잡하고 이기종 시스템을 위한 신뢰 대응과 복구에 대한 뚜렷한 진보는 없다. 그러나 인프라 측면에서 이러한 능력은 높은 수준의 중요성을 가진다.

대응과 복구 동안 시스템 행위는 예측 불가능하고 관리가 어렵다. 현재 구조에서는 대응과 복구 활동이 (침해된) 네트워크에 크게 의존함으로써, 공격자로 하여금 그러한 활동들을 감시할 수 있게 만든다. 그리하여, 손상되고 붕괴된 운영 기간동안 추가 공격에 대하여, 특히 악성 코드나 데이터의 삽입에 대하여 심각한 취약성을 제공한다.

가. 기존 연구

생존성과 IDS를 보다 능동적으로 만드는 데 대한 관심 증대가 신뢰 대응과 복구에 대한 향후 연구를 주도하고 있다. 현재 탐지 능력은 침입 발생을 나타내는 데이터를 제공하나 침입을 저지하기 위하여 충분히 일찍 조치될 수 있는 지시자(indicator)를 제공하지 못하고 있다. 현재 임박한 공격의 조기 경보를 제공하고 공격이 실제로 해를 입히기 전에 탐지되고 정지될 수 있도록 하는 예측 기술을 연구하고 있다. 데이터 마이닝 기술도 사용이 증가되고 있다. 또한 명세서(specification) 기반 침입 혹은 비정상 탐지에 대한 연구가 진행되고 있으며, 여기서는 애플리케이션 혹은 컴포넌트의 행위가 잠재적인 오용이나 침입을 나타내는 특정 행위로부터의 분산(variance)을 가지고 기술되거나 감시된다.

상황 인식과 보안사건 데이터 관리도 중요한 관심사이다. 조직으로 하여금 자원 할당 우선순위를 정하고, 중요 공격에 더욱 효과적으로 대응하고 그리고 악성 행위로부터의 손상을 제한하기 위하여 보안에 대한 COP(Common Operating Picture)를 확립하는 것이 필요하다. 이 COP 제작과 관련하여 다음과 같은 문제가 있다.

- 탐지 가능한(그리고 탐지된) 이벤트와 위협적이라고 여겨지는 활동 사이의 상호 관련(correlation)
- 센서 수와 형태가 지속적으로 증가할 때 감시 및 탐지 능력의 확장성
- 생성된 경보(alert)에서 신뢰가 확립되도록 오탐(false positive)을 감소하기 위한 비복제(de-duplication), 이벤트 상호관련과 분석
- 실시간 감시를 통하여 탐지될 수 없는 복잡한 위협 행동을 식별하기 위한 대규모 데이터 수집, 마이닝과 분석

복구 활동이 진행되는 동안 중요 자원을 온전하게 유지하기 위하여 침입 감내 시스템과 생존 가능한(survivable) 구조에 대한 연구가 있다. 현재의 초점은 운영 기능을 복구하는 데 있고, 손상된 운영이 수용 가능한 위험 수준을 여전히 유지하는 것을 보장하기 위하여 분산 보안 능력을 사용하는 데 있지 않다.

현재 미국 사설, 정부 및 학교 부문 프로젝트에서 내부 컴포넌트와 상태에 대하여 감지하고 추론할 수 있는 자동 시스템, 그리고 복구-지향 컴퓨팅에 대한 연구를 수행하고 있다.

나. 연구 영역

현재 연구는 규모, 다른 행정 및 정책 도메인 간의 조정, 혹은 정보인프라 보호의 특징인 고도로 다양한 시스템 사이의 조정 문제를 다루고 있지 않다. 다음은 정보인프라 보호의 상태를 개선하는 데 높은 상승효과를 가져올 수 있는 연구 분야이다.

• 예측/사전-사고 탐지

특별히 복잡한 시스템에 대하여, 침입 및 비정상 탐지를 위한 현재 패턴 인식(예, 시그너처 기반)을 보완하거나 대체할 수 있는 기술에 대한 연구가 필요하다. 전사적 시스템 상태의 포괄적인 상황파악을 위해 다양한 컴포넌트(네트워크, 호스트, 애플리케이션, 장치)로부터의 상호관련, 분석, 감시 혹은 상태 데이터의 제시뿐만 아니라 단일 침입/비정상 모델, 침입탐지시스템이 센서 상태를 모니터 할 수 있는 방법에 대한 연구가 필요하다.

기존 탐지 전략에 대한 특별한 문제는 프로토콜 스택을 통한 증가된 암호화의 사용이다. 의심스러운 행위를 탐지하기 위한 기술(예를 들어, 지능적 트래픽 분석)에 대한 연구가 필요하다. 게다가, 대규모 공격을 위한 준비를 나타내는 활동의 탐지에 대한 연구가 특별히 필요하다.

• 시스템들의 시스템을 위한 복구 및 재구성

침입-허용, 자기-회복(self-healing), 문맥(상황)-인식(context-aware), 혹은 자기-안정화 시스템에 대한 현재 및 계획된 연구는 시스템들의 시스템으로 확장되거나 적용될 필요가 있다. 연구 난제로 다른 대응 전략(예를 들어, 기업 내부 및 외부 통지, 손상 제한, 봉쇄(containment), 공격자 행위 관측)의 정의, 비교 분석이 있다. 특히, 가능한 빠른 시스템 능력의 복구와 안전한 상태로의 재구성 사이에 상호보완을 관리하는 데 도움을 주기 위하여, 모델 및 결정 지원 도구가 필요하다. 재구성 및 복구 메커니즘을 자동화하기 위한 방법에 대한 연구도 필요하다.

5. 역추적, 식별 및 포렌식

공격의 소스 위치 식별(identification), 공격을 개시한 개인, 그룹, 혹은 조직 식별, 공격의 실제 성질 규명 및 선정된 대응을 정당화하기 위하여 사용될 수 있는 증거 유지능력이 특별히 긴급히 필요하다.

가. 기존 연구

사고 식별 기술은 상대적으로 성숙되었으며, 사고 기원 및 사고 특성화에 대한 약간의 연구가 수행되고 있다. 예를 들어, 역추적(traceback) 부문에서, 약간의 연구가 수행되었지만 성질을 조사하는 것일 뿐 구체적인 실용적 솔루션을 생성하지 못하고 있다. IETF에서 후방향(backward) 추적에 대한 표준을 개발하기 위하여 워킹 그룹이 출발하였지만, 지금까지 인터넷 드래프트나 RFC 어느 하나도 만들지 못하였다.

나. 연구 영역

다음은 정보인프라 보호의 상태를 개선하는 데 높은 상승효과를 가져올 수 있는 연구 분야이다.

• 사고 기원 식별

패킷 주소가 위장된 상태에서 IP 패킷의 기원을 식별하는 완벽한 솔루션은 진짜 개시 시스템을 마스크하기 위한 역할을 하는 중간(intermediate) 시스템의 사용, 비-IP 기반 중간 프로토콜의 사용, 인프라 간(cross-infrastructure) 경로(예를 들어, 유선 네트워크에서 이동, 전통적인 유선 네트워크로 전이된 경로)와 같은 추가적인 복잡함을 다루어야 한다. 사고 내 이벤트 체인에서 이벤트에 대한 신뢰할 만한 타임스탬프를 할당하기 위한 기술에 대한 연구도 필요하다.

• 개시자 식별

복수의 개인에 의하여 접근 가능한 시스템, 개인 사용자를 위하여 링크가 없는 모바일 시스템 같은 경우에는 실제적인 개시자 신원을 식별하지 못할 수 있다. 그리하여, 사고 기원을 식별하기 위한 분석은 공격자 신원을 결정하기 위한 기술로 보충되어야 한다.

• 개시자 활동

특히, 사고를 분석하기 위한 조직 사이의 조정 및 다중 소스로부터의 데이터 상호관련 능력이 필요한 것으로 여겨진다.

6. 무선 보안

무선 네트워크의 독특한 점으로 인하여 무선 네트워크의 무결성과 비밀성에 대한 새로운 취약성과 보안(security) 관심이 발생하고 있다. 유선 네트워크를 위하여 개발된 솔루션들이 무선 네트워크에서 변환될 수 없거나 구현될 수 없다. 그리하여 무선 네트워크 보안을 위하여 단독적인 연구가 필요하다.

침입 탐지 및 대응, 보안정책 관리, 정책 정의를 포함하여 구성 관리에서의 새로운 진보가 대규모, 동적, ad hoc 무선 네트워크에서 증가하는 복잡성을 다루기 위하여 필요하다. 키 관리 및 신뢰관계 관리와 같은 인증 관리를 위하여 사용되는 현재 프로토콜은 무선 네트워크를 위하여 또한 불충분하다. 무선 네트워크에만 있는 공격으로 제어 채널의 포획 및 남용, 이동 유닛을 가진 트래픽을 포획하기 위하여 네트워크 셀 경계나 근처에서의 스푸핑, 무선 전력 소스에 대한 직접 공격 등이 있다. 또한 구성/보안 정책 관리를 유지하기 위하여 필요한 데이터베이스/서비스를 지향한 공격에 취약하다. 확립된 침입 탐지 기술들이 무선 네트워크에서는 문제가 된다.

가. 기존 연구

현재 미국 정부 지원 연구는 침입 탐지 및 복구뿐만 아니라 네트워크의 건강을 이해하기 위한 인증, 키 관리, 분석 도구 등이 있다. 현재 다른 연구로는 무선 네트워킹을 위한 확장성 있는 동적인 자기-구성 네트워크의 개발이 있다. 무선 네트워크를 위한 암호화, 견고성, 신규 프로토콜 부분에서도 연구가 또한 진행되고 있다.

산업체에서의 연구의 예로 802.11 네트워크를 감시하기 위한 진단 도구가 있다. 또한 산업체에서는 시스템과 정보 무결성을 개선하기 위하여 보안을 이동 컴포넌트와 하드웨어에 임베드시키는 작업을 진행하고 있다.

진행중인 연구에도 불구하고, 무선 보안의 기본적이고 하부 이론이 강조되지 않은 상태이다. 제품과 현재 연구는 보안을 무선 네트워크의 필수 컴포넌트가 아니라 불완전한 “add-on” 보안 능력으로서 제공하고 있다. 보안을 모든 프로토콜 계층으로 확장하고 보안을 무선 장치에 임베드시키기 위한 연구가 필요하다.

나. 연구 영역

다음은 정보인프라 보호의 상태를 개선하는 데 높은 상승효과를 가져올 수 있는 연구 분야이다.

• 무선 네트워크의 필수 컴포넌트로서의 보안

유선 시스템을 위하여 개발된 보안 개념과 솔루션들이 무선에 완전하게 적용될 수 없다. 유선과 무선 네트워크의 비일치성이 지속적인 보안 취약성 소스가 될 것으로 기대된다.

• 무선 보안의 기본 이론

무선 보안 이론이 초기 상태에 있기 때문에, 안전한 대규모 무선 네트워크의 모델링, 측정 및 설계를 가능하게 하는 근본적인 특성을 식별하고 이해하기 위한 연구가 필요하다.

• 무선 시스템을 위한 장비 레벨에서 보안 개발

특히, 무선 시스템을 위한 임베디드 보안과 무선 보안을 사용자에게 더욱 투명하게 하기 위한 연구가 필요하다.

• 프로토콜 레벨에서 무선 보안 연구

단기로, 무선 네트워크에서 기존 프로토콜의 보안 의미를 이해하는 데 대한 연구가 더 필요하다. 중기(mid-term) 연구는 무선 네트워크를 위하여 맞추어진 안전한 탄력 있는 프로토콜의 개발에 초점을 맞출 필요가 있다.

• 모든 프로토콜 계층 사이의 보안 메커니즘 통합

현재 보안 프로토콜은 어느 한 계층에 주로 상주

한다. 무선 네트워크 공격에 대하여 개선된 보호를 가능하게 하는 통합된 다중 계층 방어를 제공하기 위한 연구가 필요하다.

- 대형 시스템, 네트워크, 시스템의 시스템으로 무선 보안의 통합

무선 통신은 네트워크 자원의 더욱더 확산된 제어를 가능하게 하기 때문에, 네트워크에 중요한 장치의 보안이 보안 전문지식이 부족한 개인의 손에 달려 있다. 무선 노드의 보안이 사용자의 보안 전문지식 수준에 의존하지 않도록 시스템의 임베디드 보안을 개선하기 위한 연구가 필요하다.

- 언제라도 무선 네트워크의 상태를 알거나 시각화 할 수 있는 보안 상황 인식

무선 환경에서 네트워크 토폴로지는 노드가 추가되고, 이동, 제거되기 때문에 지속적으로 변한다. 간헐적인 연결성, 노드와 링크 실패, 위협도 네트워크를 적절히 특성화 하기 위하여 탐지되어야 한다. 단기로는 무선 보안의 상태를 감시하고 나타낼 수 있는 방법에 대한 추가적인 연구가 필요하다. 중기적인 초점은 공격에 대응하기 위하여 지능적인 생존성과 적응적인 연결성을 포함하여, 공격을 다루는 것에 있다.

- DDOS 공격 처리

잠재적으로 침해된 무선 노드의 식별과 봉쇄 그리고 DDOS 공격 대처에 대하여 향후 연구가 필요하다. 무선 네트워크의 방송, 동적, 이동 성질이 침해된 노드를 식별하고 고립시키는 것을 특히 어렵게 한다. 비슷하게 무선 네트워크는 DDOS의 형태에 취약하다. 대표적인 유선 네트워크에서는 위협이 되지 않는 재밍(jamming)과 하나의 소스가 복수의 무선 노드를 동시에 영향을 미치는 것이 있다.

7. 메트릭스와 모델

가. 기존 연구

정부 프로그램은 제품 평가, 일치성(compliance) 평가, 위험 평가 관점 및 사이버 보안에서 상대적 투자 평가에 대한 방법들을 제공한다. 예를 들어, 제품 평가는 CCEVS(Common Criteria Evaluation and Validation Scheme) 하의 공통 기준(Common Criteria: CC)에 대하여 수행된다. NIST는 능력 평가에 대한 안내를 제공한다.

그러나, 이 방법들의 유효성이 불충분한 정보, 운용 환경에 대한 부적절한 연결, 고립된 특성의 측정, 비즈니스 및 위험 모델에 대한 연결 결여 등에 의하여 방해를 받는다. 연구는 컴포넌트들의 특성으로부터 시스템의 특성 평가가 아니라 특정 특성의 평가에만 초점을 맞추는 경향이 있다. 정보인프라 보호 상황은 의미 있는 메트릭스(metrics)와 모델의 개발에 복잡성을 더해준다.

사이버 보안에서의 위험 평가와 의존성 모델링은 보안 시장에서 거의 힘을 얻지 못한 채 미성숙 상태로 남아 있다.

나. 연구 영역

다음은 정보인프라 보호의 상태를 개선하는 데 높은 상승효과를 가져올 수 있는 연구 분야이다.

- 분석 지원을 위한 데이터 기초의 개발

위험 분석을 위하여 타당성 있는 정보-수집 기술, 의미 있는 측정을 생성할 방법, 측정 과정의 결과를 효과적으로 통신하기 위한 방법에 대한 연구가 필요하다. 특히, 정보인프라 보호 도메인을 위한 적절한 모델을 제공하기 위하여 집단 위험 평가(population risk assessment)와 효과적인 위험 통신(risk communication)에 대한 연구가 필요하다.

- 의사 결정 지원을 위한 메트릭스와 모델

의사 결정권자에게 정보를 주는 여러 가지 형태의 분석을 지원하기 위하여 메트릭스와 지원 개념 모델이 필요하다.

  - 경제적 분석: 보안을 위한 비용-이익(cost-benefit) 모델의 정의를 위한 연구가 필요하다. 특별히 시간의 경과에 따라 비교하는 데 사용될 수 있는 비용 이익모델과 메트릭스에 관심이 있고, 모델 혹은 측정 시스템의 사용

을 지원하거나 허용하지 않는 기술과 운용 환경에 대한 가정을 나타내는 방법에 대한 연구가 필요하다. 다른 조직 구조와 프로세스(예를 들어, 집중형(centralized) 대 비집중형(decentralized) 관리, 계층형(hierarchical) 대 P2P 보고 구조, 사고 대응 절차)의 보안 의미에 대한 연구가 필요하다.

- 위험 분석: 위험 및 구성 인자(즉 위협, 취약성, 결과 및 보호)에 대한 모델과 메트릭스에 대한 연구가 필요하다. 특별히 관심 있는 것은 내부자 위협 모델과 내부자 위협 행위의 관련 측정 가능한 지시자(indicator)의 개발이다. 정보인프라 보호 관점에 구체적인 점을 다룰 필요가 있다.
- 기술적 분석: 보안 특성과 다른 형태의 정보인프라 구성요소의 의존성 모델과 메트릭스를 정의하기 위한 연구가 필요하다. 구성요소의 성질로부터 시스템의 성질을 결정하기 위한 기술이 시급히 필요하다. 이러한 것으로는 다른 정도의 충실도까지 평가되거나 모델이 될 수 있는 구성요소로부터 시스템의 합성, 대규모 평가를 위한 필요, 다른 시간에서 수집된 데이터를 결합하기 위한 필요성이 있다.

• 시뮬레이션

정보인프라의 보안-관련 행위의 시뮬레이션을 구축하기 위한 연구가 필요하다. 어떻게 취약성이 이용되고, 네트워크가 공격에 의하여 어떻게 영향을 받으며, 공격이 어떻게 인프라 상호의존성에 기초하여 전이하는지, 네트워크의 다른 부분에서 이기종 시스템과 다른 정책 실행의 영향, 다중 시스템 혹은 인프라 구역 사이에 공격이 어떻게 조정될 수 있는지를 탐구하기 위하여 시뮬레이션이 필요하다. 시뮬레이션은 네트워크 노드의 추가나 제거와 같이, 정보인프라의 동적 구성을 또한 나타낼 수 있어야 한다. 마지막으로, 시뮬레이션은 시간에 따라 진화하는 시나리오의 조사를 지원하기 위하여 시간 차원을 포함해야 한다.

8. 법, 정책 및 경제적 문제

I3P의 조사 과정을 통하여 정보인프라가 존재하고 개발되는 경제적 요인, 법, 규정 및 정부 정책이 매우 중요하다는 것이 분명해졌다.

가. 기존 연구

실제 사이버 위협과 취약성이 존재한다고 믿고 있지만, 정책 입안자, 입법자 및 결정권자에게 그것을 보여줄 이런 문제들에 대한 포괄적인 분석이 없어 왔다. 실제로 이런 문제의 중요성과 범위에 대한 회의론자가 있다. 현재 결정, 입법 및 정책 우선순위는 문제의 일부분, 일화 같은 증거 및 인상을 단지 묘사하는 통계에 기초하고 있다. 투자자들은 공공 및 개인부문 관점에서 정보인프라 보호 문제의 기저에 있는 기본적인 질문들—무엇이 가능하며 행해져야 하는가, 예상되는 조치의 효력, 누가 왜 책임이 있는가—이 연구 주제에 대한 동기가 되어야 한다고 강조하였다.

나. 연구 영역

연구에 대한 특정 영역은 다음과 같다.

• 문제 정의

정보인프라 보호를 이루는 역동성을 보다 잘 이해하기 위한 연구가 필요하다. 이는 기술뿐만 아니라 법적, 정책 혹은 경제적 요인 변화가 다른 것에 어떻게 영향을 미치는가이다. 이러한 이해가 경제적 경쟁성, 국가(national) 보안, 국토(homeland) 보안 및 공중 건강 및 안전을 적극적으로 다루는 보안 솔루션의 개발에 기초적이다. 특히, 정보인프라 보호 문제의 범위 및 크기 확립, 이에 대한 경제, 보안, 공중 건강 및 안전 영향 등에 대한 확고한 분석 연구가 필요하다.

어떤 출현 기술에 대하여, 기술과 그 가능한 사용의 보안 의미뿐만 아니라 법적, 정책 및 경제적 의미에 대한 동반 연구가 필요하다.

• 마켓 이슈

시장 구성 요소와 어떻게 여러 가지 간섭이 시장

에 영향을 미치는가에 대한 분석 기반 이해가 기본적으로 중요하다. 시장의 구조와 역동성을 묘사하기 위한 연구가 필요하다.

• 상호보완

기술적 능력과 비밀성과 시민 자유 사이에는 기본적인 상호보완이 존재한다고 믿어진다. 이러한 관심을 다루기 위하여, 보안 공공-개인 협력의 성공 한계와 가능성의 근본적인 이해의 개발 그리고 책임 법규, 투자 정책 등의 규정 및 변화와 같은 정부 간섭을 이용하는 다른 접근 방법의 의미에 대한 분석 기반 이해 개발에 대한 연구가 필요하다. 공공 및 개인부문 사이의 보안 부담 공유문제를 해석하기 위한 연구도 필요하다.

• 표준 및 일반적으로 수용되는 보안 원칙 및 실제

보안 표준의 의미 규명, 경제적 기대 영향과 책임성 의미 측면에서 가장 좋은 실제의 유효성 분석, 소유권 문제에 대한 결정을 위한 해석 기반에 대한 연구가 필요하다.

• 모델링, 메트릭스 및 데이터

보안에 대한 결정을 내리기 위하여 문제의 크기 측정을 위한 방법, 제안된 솔루션의 기대 효과, 정보인프라의 상태를 적절히 묘사하는 데이터, 그리고 문제의 역동성 이해에 도움을 주는 도구를 가져야 한다. 이것이 어떤 솔루션, 메트릭스 및 모델링 연구 주제에서 특별히 중요한 구성 요소이다. 모델링과 포렌식 업무를 성취하기 위하여 어떤 데이터가 필요하며, 비밀성과 시민 자유와 같은 다른 문제점들에 대한 수집의 의미, 누가 수집해야 하는가, 얼마나 오래 보존되어야 하는가와 같은 문제들에 대한 연구가 필요하다.

• 직접 대응

마지막 관심은 “역 해킹(hack back)” 혹은 “능동 방어”라고 알려진, 공격에 대한 직접 대응이다. 많은 악성 행위들이 외국을 경유하여 발생하거나 통과하기 때문에 이러한 외국 엔티티에 대한 조치를 허용하는 정책이나 법규가 국제적으로 중요하다. 게다가, 공격을 수행하는 데 사용된 체인의 마지막 서버가 아니라, 사실상의 공격자를 적절히 식별하는 기술적인 어려움이 이 문제를 더욱 모호하게 한다.

주어진 상황과 의미에서 직접 대응을 허용하는 법규나 정책에 대한 변화의 잠재적인 가치의 이해 개발에 대한 연구가 필요하다.

IV. 요약 및 맺음말

위의 절에서 살펴본 신규 및 부가적인 연구가 필요한 각 영역에 대한 요약은 아래와 같다[11].

• 통합 보안 관리(Enterprise Security Management)

이 영역에서 어려운 문제는 다양한 보안 메커니즘들을 통합 자원에 대한 접근을 관리하고 사용하기 위하여 일관성 있는 능력으로 통합하고, 통합 시스템상의 행위 모니터링, 의심스러운 혹은 비적합 행위의 탐지 및 대응이다. 통합 정책 정의 및 관리, 목표된 위험 형국의 정의 및 유지관리, 보안 경계의 정의 및 경계에서의 보호 부문에도 더 많은 연구가 수행되어야 한다. 내부자 위협에 대하여도 향후 연구가 필요하다.

• 분산 자율 파티 사이의 신뢰

지역적으로 혹은 조직적으로 분산된 자율 엔티티(즉, 개인, 조직, 소프트웨어 및 장치 등을 말함)를 위한 트러스트 모델, P2P 설정에서 동적인 보안 관계의 정의 및 관리, 시스템과 셀 전화기 혹은 랩 톱과 같은 종단 사용자 장비 사이의 트러스트 관계를 개발하기 위한 기술, 데이터 신뢰성 확립 방법에 대하여 연구 필요성이 존재한다.

• 보안 특성과 취약성 발견 및 분석

정보인프라는 하드웨어, 펌웨어, 소프트웨어, 통신매체, 저장매체 및 정보와 같은 다른 형태로 많은 수의 다양한 컴포넌트를 가지고 있다. 제품 및 시스템들은 통상적으로 취약성과 부적절하게 이해된 보안 성질을 포함한다. 더욱이, 한 시스템 혹은 하부시스템의 보안 성질은 컴포넌트들로부터 유도되거나

유추될 수 없고, 대규모 시스템에서 나타나는 성질은 기술하기 어렵고 예측하기가 힘들다. 제품이나 시스템의 수명 주기를 통하여 이용 가능한 결점이 도입되었는지 혹은 예측하지 못한 보안 성질이 나타났는지의 여부에 대하여 결정하기 위한 방법에 대한 필요성이 절실하다. 동적이고 대규모 환경에서 코드, 장치 및 시스템을 분석하기 위한 기술에 대한 연구도 필요하다.

• 안전한 시스템과 네트워크 대응 및 복구

공격으로부터의 생존성과 침입탐지시스템을 보다 능동적(proactive)으로 만드는 능력이 안전한 대응과 복구에 대한 연구를 주도하게 만들었다. 그러나 현재 연구는 규모 문제, 다른 행정 및 정책 도메인 사이의 조정, 혹은 고도로 다양한 시스템 사이의 조정에 대하여 적절히 다루지 않고 있다. 시스템들의 시스템을 위한 복구 및 재구축뿐만 아니라, 예측 혹은 사전-사고 탐지 부문에 대한 연구 필요성도 존재한다.

• 역추적, 식별 및 포렌식

대응자의 공격 역추적, 공격 소스 위치 식별, 공격을 개시한 개인, 그룹, 혹은 조직의 식별, 공격의 실제 성질을 결정하기 위한 능력에 대한 연구 필요성이 존재한다. 이런 능력의 법적인 그리고 정책 의미를 다루기 위한 동반 연구도 필요하다.

• 무선 보안

실제로 유선 네트워크를 위하여 개발된 솔루션이 무선 환경에서 실행 가능하지 않다. 보안을 무선 네트워크의 필수적인 컴포넌트로 만들고, 무선 보안의 기초과학 개발, 무선 장비 자체에 통합 가능한 보안 솔루션 개발, 기존 무선 프로토콜의 보안 의미 조사, 모든 프로토콜 계층 사이의 보안 메커니즘 통합, 무선 보안의 대형 시스템과 네트워크로의 통합에 대한 연구가 필요하다. 특히, 무선 네트워크에 대한 보안 상황인식 기술과 분산 서비스 거부 공격을 다루기 위한 전략에 대한 연구가 필요하다.

• 측정 기준과 모델

조직의 임무와 전략에 관련될 수 있는 투자 결정을 위한 분명한 기반을 제공하기 위하여, 사이버 보안을 위한 엄격하고 일반적으로 수락된 모델과 측정 기준(메트릭스)에 기초하여야 한다. 현재 투자와 위험 수준에 대한 자료의 기초를 제공하기 위한 연구가 필요하다. 또한 경제적, 조직, 기술적 및 위험과 같은 여러 가지 관점에서 보안 관제의 비용, 혜택, 영향을 나타내는 측정기준에 대한 연구도 필요하다. 정보인프라의 보안-관련 행위를 모델링하고 위험 관리 선정의 결과를 예측하기 위한 기술에 대한 연구도 필요하다.

• 법, 정책 및 경제적 문제

정보인프라의 보안에 영향을 미치는 결정들이 경제 요인, 법, 규정 및 정부 정책을 잘 이해하지 못한 상황에서 이루어진다. 사이버 보안 문제의 실제 크기를 결정하고 정보인프라 보호를 형성할 세력 사이의 관계를 잘 이해하기 위한 연구가 필요하다. 즉, 시장 구조, 기술 및 법, 정책, 경제 여건의 변화가 어떻게 서로 영향을 미치는가에 대한 연구가 필요하다. 출현 기술에 대하여, 그 기술의 보안 의미와 가능한 용도뿐만 아니라 법적, 정책 및 경제적 의미에 대한 동반 연구도 필요하다.

카네기 멜론대의 CERT 센터는 현재 컴퓨팅 환경에 영향을 주는 6가지의 최근 공격 동향을 아래와 같이 확인하였다.

- 현재 공격 도구 세대에서 증가된 자동화 수준
- 공격 도구의 정교화
- 시스템 취약성의 빠른 발견 및 보고
- 방화벽의 증가된 침투성
- 공격과 결과의 증가된 비대칭
- 인프라 공격으로부터 위협 증가

이와 비슷하게 최근 해킹 동향으로 해킹과 바이러스 기술의 통합화, 인프라 공격의 증대, 해킹 매체 및 목적의 다양화, 해킹 기술의 고도화 등을 제시하고 있다[4]. 이와 같은 추세에 따라 차세대 정보보호 기술로 여러 가지 분야에서의 보안 기술 발전이 요구되고 있는 실정이다. 이러한 요구에 따라, 본 고에서는 미국의 I3P의 보고서 내용을 중심으로 미국

의 정보인프라 연구개발 방향과 기술에 대하여 고찰하고 제시하였다.

이 R&D 목록 개발과정의 참여자들은 연구분야의 식별과는 관계없으나, 보안의 실천에 영향을 미치기 위하여 궁극적으로 방법을 탐구하는 연구자들을 위한 중요한 고려사항의 필요성이 중요함을 제시하고 있다[11]. 이러한 것들로 교육, 훈련과 인지, 품질보증 방법론, 정보 공유 및 조정, 실천 가능한 절차, 물리적 보안 등이 있다. 비슷하게, 기술 전수도 빈번하게 문제점으로 지적되었다. 잠재적으로 가치 있는 연구결과가 제품이나 시스템에 반영되지 못하고 있다는 지적이다. 연구자, 제품 개발자, 시스템 통합자 및 종단 사용자 조직 사이의 아이디어와 기술의 흐름을 개선하기 위한 전략에 대하여 유의가 보다 필요하다는 지적이다.

참 고 문 헌

[1] U.S. Department of Homeland Security, Protecting Cyberspace, http://www.nipc.gov/.

[2] 전황수, “미・일의 정보보호대책과 우리에게 주는 시사점,” 주간기술동향 통권 1092호, 2003. 4. 22., pp.15-29.

[3] 전자신문, 10면, 정보화 솔루션, 2004. 3. 19.

[4] 서동일, “최근 정보보호 기술 개발 동향 및 전망,” 발표자료, 한국전자통신연구원, 2003. 12. 22.

[5] 심원태, “네트워크 보안기술 전망,” 발표자료, 정보통신연구진흥원, 2003. 9. 25.

[6] 오승희, 남택용, 손승원, “네트워크 보안 기술 동향,” 주간기술동향 통권 1116호, 2003. 10. 7., pp.1-14.

[7] 이윤철, “정보보호 제품동향 및 세계시장 현황,” 주간기술동향 통권 1108호, 2003. 8. 13., pp.28-41.

[8] 이윤철, “전세계 정보보호 및 Business Continuity 시장동향,” 주간기술동향 통권 1127호, 2003. 12. 24., pp.31-42.

[9] 황성원, “국내 정보보호 현황과 발전방향,” 정보통신연구진흥지 통권 15호, 정보통신연구진흥원, 2003. 3.

[10] I3P(Institute for Information Infrastructure Protection), Cyber Security Research and Development Agenda, Jan. 2003.

[11] I3P(Institute for Information Infrastructure Protection), National Information Infrastructure Protection Research and Development Agenda Initiative Report, Information Infrastructure Protection: Survey of Products, Tools, and Service, Ver. 1.0, Sep. 2002.