정보통신 인프라 보호를 위한 미국의 연구개발 동향

대구가톨릭대학교 컴퓨터정보통신공학부 전용희
한국전자통신연구원 정보보호연구단 손승원

차 례

1. 서 론

2003년 1월 25일 '인터넷대란'이 발생한 이후 국내에서도 정보인프라 보호(Information Infrastructure Protection: I2P)에 대한 관심이 증대되었다. 그 결과의 일부로 올해 3월 18일 세계적인 보안 업계인 시만택의 '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[10].

미국정부는 2002년 7월 각종 위협으로부터 본토의 안전과 자국민의 보호를 위한 목적으로'Homeland Security' 계획을 발표한 바 있다[3]. 또한 같은 해 9월 안전한 사이버공간을 위한 국가전략(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. 또한 다음과 같은 5 가지의 사이버보안 우선 영역을 설정하였다.

- 사이버보안 대응 시스템 개발
- 위협 및 취약성 감소 프로그램의 생성
- 인식 및 훈련 프로그램의 생성
- 정부 컴퓨터를 보호하기 위한 계획 공개
- 국가 안보와 국제 협력을 상세히 기술하는 계획 개발

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 자국민

에 대한 보호를 강화하고, 생화학이나 핵무기 등에 의한 공격 등 물리적인 위협뿐만 아니라 사이버위협에 대한 대비를 강구한 의의가 있다[11].

국내에 정보보호 제품, 기술 개발 및 연구 동향을 소개하는 약간의 문헌이 존재하나, 정보인프라 보호에 대한 연구개발 동향을 폭넓게 소개하는 문헌은 아직 존재하지 않고, 더구나 연구개발 분야에 대하여 보다 자세한 내용 기술이 필요하다고 사료된다[4-9,12]. 이에 따라 본고에서는 정보보호 수준이나 대응체계가 훨씬 앞서있는 미국의 정보통신 인프라에 대한 연구개발 동향을 고찰하여보고 향후 국내의 정보통신 인프라 보호 연구개발 방향 정립에 기여하고자 한다. 본고에서는 미국의 I3P(The Institute for Information Infrastructure Protection)의 보고서 내용을 중심으로 미국의 정보통신 인프라 보호 연구개발 동향에 대하여 주요 기관별로 기술한다[1,2].

2. I3P

2.1 개요

I3P는 사이버 보안과 정보인프라 보호 연구개발에 초점을 맞춘 23개의 학교 및 비영리 연구조직의 콘소시엄으로 구성되어 있으며, 본 절에서는 미국 내의 사설 부문 및 정부 지원 연구활동의 집합체에 의한 정보 인프라의 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.

- 생존성(survivability): 공격에 저항하고, 중요한 서비스를 회복하고 안전한 상태를 재구성하여 생존 능력을 가지고 운용을 계속하는 시스템 능력을 말한다.
- 평가력(assessability): 복잡한 분산 시스템이 자신의 보안 상태와 배열을 평가하고, 보안 관련 특성을 모델링하고, 측정하고, 비교할 수 있는 기술을 조사할 수 있는 능력을 말한다.
- 구성력(composability): 지역 및 원격 엔티티를 포함하여 시스템 컴포넌트 간에 확장 가능한 방법으로 보안을 반영하고 보안 보증을 목표로 하는 기술을 말한다.
- 자동, 실시간 대응: 이벤트 발생에 따라 공격을 자동적으로 실시간 대응하고, 공격자 추적 및 시스템 포렌식(forensics)까지 포함하기 위하여 대응을 확장하는 능력
- 자기-강화 시스템: 높은 척도의 시스템 자기-인식, 자기 평가, 자연적이고 적대적인 비계획된 이벤트에 대한 적응성을 성취하기 위한 시스템.

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

- 암호술(cryptography): 암호술 연구의 가장 강한 두 분야는 아래와 같다.
  - 대표적인 PKI 애플리케이션에서 암호화를 하위 계층 네트워크 장치로 임베드하는 쪽으로 암호기술의 확장
  - 양자 레벨 암호술의 증가된 연구
- 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 능력

· 안전한 배치(구성) 및 시스템 보증: 시스템에게 보안 상태를 동적으로 평가하고 변경하기 위하여 자신의 보안 배치와 능력에 대한 지식을 부여하기 위한 연구에 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 신빙성: 이 연구 분야는 주 연구 주제는 아니지만, 진보된 부인 방지와 신빙성 기술이 시스템 자기-인식과 자기-평가에서 요소로 나타나고 있다. 디지털 저작권 관리(DRM: Digital Rights Management) 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 연구 영역이다.

2.2 영역별 연구 현황

I3P 보고서에서 확인된 연구 영역은 8개 분야이다. 아래에서 각 영역별로 요약하여 기술한다.

• 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 유지 관리, 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 신뢰(trust) 모델, 피어 투 피어(P2P) 세팅에서 동적인 보안 관계의 정의 및 관리, 시스템과 셀 전화기 혹은 랩톱과 같은 종단 사용자 장비사이의 신뢰 관계를 개발하기 위한 기술, 데이터 신뢰성 확립 방법에 대하여 연구 필요성이 존재한다.

• 보안 특성과 취약성 발견 및 분석

정보인프라는 하드웨어, 펌웨어, 소프트웨어, 통신매체, 저장 매체 및 정보와 같은 다른 형태로 많은 수의 다양한 컴포넌트를 가지고 있다. 제품 및 시스템들은 통상적으로 취약성과 부적절

하게 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 기초 과학 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 상황 인식 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 측정기준(metrics)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. 정보 인프라의 보안-관련 행위를 모델링하고 위험 관리 선정의 결과를 예측하기위한 기술에 대한 연구도 필요하다.

• **법, 정책 및 경제적 문제**

정보 인프라의 보안에 영향을 미치는 결정들이 경제 요인, 법, 규정 및 정부 정책을 잘 이해하지 못한 상황에서 이루어진다. 사이버 보안 문제의 실제 크기를 결정하고 정보 인프라 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.

3. ICI

미국 ICI(Information and Communications Infrastructure) 보고서는 4 개의 연구 범주 안에서 13 개의 연구 개발 필요성을 정의한다. 연구 범주는 다음과 같다.

- 위험, 위협, 취약성
- 침입자 및 사고 탐지 대응 및 복구
- 고-신뢰 인프라 공학
- 모델링 및 시뮬레이션 도구

3.1 위험, 위협, 취약성

다음은 위험, 위협, 취약성에 대한 R&D 주제별 로드맵을 보여준다.

1) 취약성 탐지 및 분석

- Near Term: 취약성 정보 수집, 분석, 분류 절차 개발
- 2005년까지 성취:
  - 인프라에 대한 취약성 정보를 식별하기 위한 어휘와 데이터베이스 개발
  - 취약성을 탐지하고 분석하기 위한 도구의 유효성을 측정하기 위한 측정기준 및 측도 개발
  - 취약성 탐지 도구 자동화
- 2010년까지 성취:
  - 국가적 수준에서 취약성 탐지 및 데이터 통지를 위한 조정되고 확장 가능한 도구의 개발
  - 취약성 정보 수집 및 공유를 위한 국제적 협력 확립

2) 정보의 가치평가

- Near Term: 정보 가치를 평가하기 위한 수동적 도구, 기술, 절차 개발
- 2005년까지 성취: 정보 가치를 평가하고 적절한 수준의 보호를 결정하기 위한 자동화 도구의 개발
- 2010년까지 성취: 다중 소스로부터 집합될 수 있는 정보를 포함하여, 정보와 보호의 가치를 평가하는데 도움을 주는 자동화 도구의 개발 및 정련

3) 위험 분석

- Near Term: 반자동 위험 분석 도구 개발 및 위험 평가 기술과 측정기준 정형화
- 2005년까지 성취: 구성 요소 변경 시 시스템과 네트워크에 대하여 동적으로 위험을 평가하기 위한 자동화된 위험 분석 도구 설계
- 2010년까지 성취: 신기술의 출현과 시스템 구성요소를 반영하기 위하여 진보된 자동 위험 분석 도구 개발

4) 위협 특성화와 통지

- Near Term: 위협 데이터 수집, 분석, 분류 절차 개발
- 2005년까지 성취:
  - 위협 및 대응 정보의 국가 데이터베이스 구현
  - 잠재적 공격자 프로파일
- 2010년까지 성취:
  - 위협 통지를 위한 조정된 국가 수준의 도구 개발 및 분배
  - 위협 데이터 수집 및 공유를 위한 국제적 협동 확립

3.2 침입과 사고 탐지, 대응 및 복구

다음은 침입과 사고 탐지, 대응 및 복구에 대한 로드맵을 보여준다.

1) 침입과 사고 탐지 및 경고

· Near Term:
  - 사고 탐지 및 경고 발생을 위한 수동 도구 및 절차 개발
  - 침입탐지시스템 평가를 위한 측정기준 확립
· 2005년까지 성취: 사고 탐지 및 경고 발생을 위한 자동 도구, 전략-기반 침입탐지시스템, 자동 역추적 도구, 확장성 있는 탐지 시스템 개발
· 2010년까지 성취:
  - 공격 지시 및 경고를 탐지하기 위하여 국가 수준에서 확장성 있는 도구 개발
  - 공격에 대한 국제적 협력과 데이터 공유 확립
  - 인터넷 위협을 평가하기 위한 확장성 있는 평가 도구 생성

2) 대응, 복구 및 재구성

· Near Term: 침입자의 탐지, 포획, 방출 그리고 공격된 시스템 상의 복구를 위한 분류를 수행하는 수동 도구 개발
· 2005년까지 성취: 침입자의 탐지, 포획, 방출 그리고 공격된 시스템 상의 복구를 위한 분류를 수행하는 자동 도구 개발
· 2010년까지 성취: 견고성, 효율성, 복구의 시의 적절한 대응을 개선하기 위한 자동 도구의 개발 지속

3.3 고-신뢰 인프라 공학

다음은 고-신뢰 인프라 공학의 로드맵을 보여준다.

1) 보안 구조

· Near Term:
  - 보안 패치의 자동 분배를 위한 방법론 확립
  - 보안 구현 정책 준비
· 2005년까지 성취: 진보된 방화벽 기술과 능동, 동적 네트워크 기술 개발
· 2010년까지 성취: 보안 구성 요소 통합을 위한 확장성 있는, 견고한 보안 구조 개발

2) 보증 기술

· Near Term: 표준과 시스템 개발과 완전한 제품 평가 정책으로 보증을 반영하는 방법 확립
· 2005년까지 성취: 효율적인 제품 평가 및 시스템 수준 평가를 위한 도구 개발
· 2010년까지 성취: 보증을 시스템 개발에 반영하기위한 방법론과 기술의 지속적인 개발과 정련

3) 진보된 개념과 이론

· Near Term: 소프트웨어 개발을 위한 표준, 기술, 절차 확립
· 2005년까지 성취: 네트워크 관리에서 전문가 시스템을 사용하고, 시스템을 적응적으로 안전하게 하기 위한 방법 연구개발
· 2010년까지 성취: 자기-묘사 신뢰 시스템 개발

4) 정보보호 관리

· Near Term:
  - 데이터 보호 및 지역과 원거리 인프라 구성요소에서 구성 관리를 수행하기 위한 개념과 기술의 연구개발
  - 정보 보호 평가를 위한 성능 측정기준 정의
· 2005년까지 성취:
  - 사용 조건이나 정보와 함께 메타데이터를 수반하는 정보 보호 개념 연구

- 정보 보호 평가를 위한 경제적 측정기준 확립
- 2010년까지 성취: 다양한 환경에서 데이터 보호 관리를 위한 측정 개념, 도구 및 기술의 지속적인 개발과 정련

5) **필수 서비스를 위한 최소 인프라의 특성화**

- Near Term: 최소의 필수적인 정부 및 군 통신, 운영과 서비스, 서비스를 지원하기 위한 요구 인프라 정의 및 특성화
- 2005년까지 성취: 기관 사이의 비상 및 조정 계획 확립, 중요 응용에서 잉여 시스템의 도입 처리
- 2010년까지 성취: 신기술이 출현하고 정부 서비스 범위가 발전함에 따른 잉여성을 보증하기 위하여 계획을 수립하고 부가적인 기술 전개

6) **암호화 기술**

- Near Term: 보안 키 관리를 위한 국가 표준 확립
- 2005년까지 성취: 강건한, 고성능의 비용 효율적 암호 기술 개발
- 2010년까지 성취: 컴퓨팅 파워의 상당한 증가가 이용 가능하면 강건한 암호화 기술의 지속적인 진보 및 정련

3.4 인프라를 위한 모델링 및 시뮬레이션 도구

다음은 인프라를 위한 모델링 및 시뮬레이션 도구 로드맵을 보여준다.

- Near Term: 소규모 네트워크 시스템에 대한 요구사항 정의 및 모델링과 시뮬레이션 개시
- 2005년까지 성취:
  - 구조 레벨에서 복잡한 시스템을 모델링하기 위한 도구 및 모델 개발
  - 시스템 내 상호의존성 및 취약성을 모델링하기 위한 도구 및 기술 개발
- 2010년까지 성취: 구조 레벨에서 시스템 사양서와 편차를 탐지하기 위한 자동 도구, 자기-묘사 시스템을 위한 기술 및 사양서 개발

4. IRC

IRC(INFOSEC Research Council)는 DoD, IC 및 FDA(Federal Civil Agencies)로부터의 정보 보안 연구의 미국 정부 후원자로 구성된다. IRC는 학교, 정부, 산업 R&D 프로그램을 상호 이익을 위하여 더욱 통일되고 효과적인 방법으로 영향을 주기 위하여 효과적인 방법을 제공한다. "HPL(Hard Problems List)"은 솔루션이 효과적인 정보 보안에 대하여 주요한 장애를 제거할 수 있는 핵심 문제를 식별하여 연구 프로그램 기획을 지도하기 위함이다.

HPL 로드맵의 보안 특징은 다음과 같다.

- 침입 및 오용 탐지: 컴퓨터 시스템과 네트워크의 침입과 오용을 탐지하고 국소화하기 위한 도구
- 침입 및 오용 대응: 침입/오용에 대응하는 도구 및 기술
- 외부 및 이동 코드의 보안: 수락할 수 없는 시스템 취약성의 개방 없이 외부 및 이동 코드 기술의 사용 능력
- 민감한 정보의 통제된 공유: 권한이 부여된 사람 사이 필요한 공유를 제한하지 않고 분류된 정보의 효과적인 통제
- 애플리케이션 보안: 애플리케이션 사용자를 위한 안전한 정보 처리 제공
- 서비스 거부: DoS 공격의 예방 혹은 저항

· 통신 보안: 트래픽 플로우 보안을 포함하여, 군사/정보(intelligence) 등급 통신 보호
· 보안 관리 인프라: 대규모 분산 시스템에서 보안 메커니즘 관리 능력
· 이동 전쟁을 위한 정보 보안: 병참 및 정보에 대한 연결성 이외에, 전술적 전쟁에서 육지, 바다 및 공중 노드 간의 개선된 안전한 연결성

5. DARPA

5.1 보안 프로그램

2000-2002에 발표된 DARPA를 위한 보안 안건(security agenda)은 다음과 같은 프로그램들을 포함하고 있다:

· Advanced Technology Office(ATO) 프로그램 안건
  - CHATS(Composable High Assurance Trusted Systems) 프로그램
  - 사이버 패널 프로그램
  - 동적 협동 프로그램
  - 결함-허용 네트워크 프로그램
· 정보 인지 사무소(IAO: Information Awareness Office) 프로그램 안건
· 정보 처리 기술 사무소(IPTO: Information Processing Technology Office) 프로그램 안건, 특히 OASIS(Organically Assured and Survivable Information Systems) 프로그램 및 OASIS 시연 및 검증(DEM/VAL: Demonstration and Validation) 프로그램
· 다른 관련 프로그램
  - 공군 연구 실험실(AFRL: Air Force Research Laboratory)에 의하여 운영되는, 정보 보증 및 생존성 진보 기술(ATIAS: Advanced Technologies for Information Assurance and Survivability) 프로그램
  - IPTO에 의하여 운영되는, DASADA(Dynamic Assembly for System Adaptability, Dependability, and Assurance) 프로그램
  - 전술적 기술 사무소(TTO: Tactical Technology Office)에 의하여 운영되는, UltraLog 프로그램

OASIS는 외부의 공격에 대한 피해를 취소화하여, 어떠한 상황에서도 일정 수준 이상 시스템의 동작이 보장되는 정보 시스템의 개발이 목적이며, 이를 위하여 다양한 취약 요소를 극복할 수 있는 침입 감내 시스템의 개발, 악의적인 코드의 복제로 인한 피해 방지, 악의적인 이동코드의 실시간 탐지; 오류 탐지, 감내, 복구, 치료 기술 개발; 침입 감내 메커니즘의 평가 및 조정 방법론의 개발을 목표로 하고 있다[4].

5.2 로드맵

DARPA의 로드맵은 다음과 같다.

· CHATS: 코어 시스템과 네트워크 서비스가 악성 코드와 다른 공격 기술이나 방법의 유입이나 실행으로부터 자신을 보호하도록 하여주는 도구나 기술. 도전 과제는 다음과 같다.
  - 개방 소스 운영 체제 사이의 증진된 보안과 호환성
  - 시스템 구성과 관리 도구 및 방법
  - 개방 소스 시스템 용 보안 감사, 분석, 시험, 서류화
  - 보안 정책, 보안 서비스, 긴요한 애플리케이션 및 하드웨어 지원
  - 보증 방법 및 도구
· 사이버 패널: 사이버 공격의 징후에 대하여 감시함으로써 중요 정보 시스템을 방어하

는 능력, 발생하는 공격 상황을 피하고 대처하기 위하여 운영자가 시스템 보안의 운영이나 생존성 특성 관리 허용 능력

- 동적 협동: 중요 네트워크 서비스의 결함 허용 및 생존성 확보, 공격자의 자원 소비를 제한하는 서비스 거부 공격 저지, 가능한 소스에 인접하게 공격을 추적하고 억제하기 위한 기술.
- 결함 허용 네트워크: 무결성 및 가용성을 강조하며, 네트워크 레벨에서 가능한 공격에 대항하여 결함 허용 능력 도입에 의한 네트워크 강화 기술, 임무-주도 협동의 동적 생성과 관리에 연관된 잠재적 취약성 완화 기술
- IAO 초점:
  - 초대규모 모든 소스 정보 저장소 용 기술 및 관련 비밀성 보호 기술
  - 인간과 기계가 복잡한 시스템에 대하여 더욱 효율적이고 효과적으로 함께 생각할 수 있도록 허용하는 협동, 자동화, 인식 보조 기술
  - 기존 DARPA 프로그램으로부터의 기술과 구성요소를 통합하여 예방을 통한 테러리즘 대처 지원 종단 간 폐회로 프로토타입 시스템
- IPTO 초점: 특히 사이버 공격에서 생존하기 위하여 설계된 구조와 관련하여, 생존가능 시스템 구조 및 상응하는 보증 논증
- ATIAS: 정보 보증(IA) 및 생존성에서의 중요한 문제에 대한 효과적인 안정된 내구성 있는 솔루션을 개발하기 위하여 설계된 공격적, 단기 연구 지향 프로그램
- DASADA:
  - 임무 중요 시스템이 DOD의 높은 보증, 의존성 및 적응성 요구사항을 만족할 수 있도록 하는 연구, 개발과 기술 전수
  - n-tier 시스템을 위한 복잡한 소프트웨어 구조로 인한 시스템 구성요소에서의 현재 결점 처리
  - 실행 중 데이터 수집을 위한 조사에 크게 기반 하는 구조-주도 접근
  - 조사 데이터를 시스템 튜닝에 의미 있는 측정으로 변환하기 위한 척도
- UltraLog:
  - 분산 에이전트 소프트웨어 구조를 충분히 안전하고, 강건하고, 확장 가능하게 만들기 위한 방법

6. 기타 기관

기타 기관으로 NIST와 NSF의 정보보호 연구개발 동향을 간략히 살펴본다[13].

6.1 NIST

미국 표준화 기관인 NIST(National Institute of Standards and Technology)에서는 ATP(Advanced Technology Program)에서 다음과 같은 정보보호 관련 프로젝트를 수행하고 있다.

- 암호: 기초 기반 기술보다는 응용을 위한 연구 방향이 주를 이루며, 인터넷에서 XML(eXtensible Markup Language) 암호화에 대한 연구를 진행하여, 인터넷을 위한 새로운 데이터 보안 모델의 프로토타입을 개발하고 있다.
- 인증: 얼굴이나 음성과 같은 생체 인식 관련 연구가 주를 이루며, 식별 기술에서 90%의 정확한 생체 인증을 수행하기 위해 개인들과 데이터 수집에서 정규 편차(normal variation)를 제공하는 신호처리 기술을 개발 시험하는 연구가 진행되고 있다. 그 외에 차세대 생체 인식 기술로 열적외선

이미징을 이용한 생체 인식 기술 개발을 수행하고 있다.

- 시스템: 신뢰성 있는 정보 시스템, 알려지지 않은 새로운 침입 유형이나 바이러스에 대하여 정보시스템이 능동적으로 대응할 수 있는 시스템에 대한 연구가 진행되고 있다.
- 네트워크: 가용성, 생존성 차원의 실용적인 연구, 인프라의 안정성과 보안성 강화 연구, 모바일, 에드 혹 등 무선 네트워크에 대한 보안 적용 연구가 주를 이루고 있다. 또한 신경망 기술을 네트워크 보안에 접목시키고자 연구가 진행되고 있다.
- 응용, 서비스: 디지털 컨텐츠 보안 방식, 전자 메일 보안 그리고 안전한 B2B를 위한 프레임워크, 데이터베이스 보안에 대한 연구를 중심으로 진행되고 있다.

6.2 NSF

NSF(National Science Foundation)의 CISE(Computer and Information Science and Engineering) 부서에서 수행하고 있는 연구 분야는 다음과 같다:

- 암호: 기존 연구와는 다른 보다 복잡한 공격 모델과 오브젝트 기반의 컴포넌트 구조를 지원하며, 이 시스템을 암호 프로토콜을 위한 컴포넌트 라이브러리 개발에 응용한다.
- 인증: 이 분야의 뚜렷한 연구 계획은 보이지 않는다.
- 시스템: 안전하고 신뢰성 있는 정보 시스템 개발을 위하여, 이 분야에는 크게 4개의 프로젝트가 있다. 침입 상호관련성 규명을 위하여, 하나의 침입탐지시스템이 가지는 불완전함을 다른 침입탐지시스템의 도움으로 개선하기 위하여 다중 결과의 일관성 있고 종합적인 방법을 그래프 이론을 바탕으로 개발하고 있다. 출판-구독(publish-subscribe) 시스템 보안 구조 연구를 위한 보안 아키텍처 설계와 시뮬레이션 기술이 개발되고 있고, 고도의 신뢰성이 있는 소프트웨어 기반 시스템을 설계, 시험, 구현, 배치 및 검증하는 능력을 목표로 NASA 테스트베드 상의 실험을 통하여 연구 결과를 평가하고 있다. 마지막으로 전자 상거래 등 많은 분야에서 진정으로 신뢰할 수 있는, 안전한 신뢰 시스템을 위하여 DoS를 방어하고, 중앙 인덱스 없이 원하는 정보를 검색하고, 인증하고, 정보 보존 문제를 해결하고자 하고 있다.
- 네트워크: 현재 사이버 인프라의 취약성 분석을 통한 보안성 강화와 미래에 보다 보안성이 강화된 네트워크를 위하여 핵심 기술에 대한 연구가 수행되고 있다. 기존의 도구로는 개별적 취약성을 찾을 수는 있으나 다중 취약성에 의한 복합적 영향을 알아내지 못하기 때문에 취약성과 탄력성 분석으로 네트워크 보안을 개선하고자 한다. 사이버 공격에 탄력성을 가지는 네트워크를 설계하고, 안전한 co-processing과 p2p 기술을 결합하여 분산 생존성 있는 신뢰 백본을 도출하고자 한다. 그리고 센서, 센싱 시스템 설계, 개념 정리 및 유무선 센서 네트워크 기술 연구와 센서 데이터 기반의 응용 개발이 이루어지고 있다.

7. 동향, 문제점 및 갭

I3P 보고서에서 동향, 문제점 및 갭은 다음과 같은 네 가지 영역으로 통합되었다: 시간-단계 로드맵, R&D 주제 로드맵, 문제 공간, 제휴(partnership)

〈표 1〉 I3P의 시간 로드맵

Focus Area	시간 프레임	주요 범주
국가(National)	Near-term By 2005 By 2010	위험, 위협, 취약성 탐지, 대응, 복구 고-신뢰 인프라 M&S 도구 설계
정부 공동체 (공군)	Near-term 2004-2007 >2007	보호 탐지 React Cyber Situation Awareness
과학 공동체 (에너지 성)	다음 5년간	6가지의 가장 중요한 영역: - 위협의 특성화 및 통지 - 탐지, 분석, 방지 - 보안 구조의 정의 - 대응, 복구, 재구성 - 진보된 이론 개념 - 정보 보호 관리
기술 (핵심 관리 인프라)	2002-03 2004-06 2007-09 2010-11 2012-13 1204-15	각 6개의 증분은 다음 범주를 포함 한다: 능력, 구조 특성, 종단 암호 단위 관리
기술 (포렌식 연구)	2001-2004	디지털 포렌식 과학 프레임워크 디지털 증거의 신뢰성 숨은 데이터의 탐지 및 복구 네트워크 포렌식스
기술 (내부자 위협 완화)	< 6 개월 6-24 개월 > 24 개월	정책 및 전략 주도 개인 관리 및 보안 훈련 및 인식 억지(deterrence) 보호 탐지 반응 및 대응

7.1 시간-단계 로드맵

6 개의 문서가 시간-단계 로드맵을 포함하고 있으며, 이 로드맵은 국가(6 기관), 정부 공동체(3 기관), 과학 공동체(4 기관) 및 특정 기술(3 기관)과 같이 네 가지 영역으로 분산된다. 표 1은 I3P의 시간 로드맵을 보여준다.

여기서 해결해야 할 과제로는 다음과 같은 것이 있다.

- I2P를 위한 R&D 로드맵을 비교, 평가, 통합하기 위한 공통 포맷, 용어, 시멘틱스
- 모든 커뮤니티를 위한 I2P 로드맵
- 가장 상위 레벨에서 비전 원칙, 비전을 이루기 위한 능력, 마지막으로 능력을 구현하기 위하여 필요한 R&D 기술을 다루는 구조적 집합의 로드맵
- 기존 갭의 분명하게 표현된 집합을 가지고

잘 정의된 문제 공간으로 사상하는 로드맵
- 능력 혹은 기술의 전개를 위한 전이 전략을 포함하는 로드맵

7.2 R&D 주제 로드맵

국가적인 연구 주제에 대한 입력은 55개 범주로 분산되어 있으며, 가장 보편적으로 식별된 범주는 다음과 같다.

- 대응, 복구, 재구성
- 구조
- 모델링과 시뮬레이션 도구

55개의 범주 중에서 접근 통제, 암호화 기술 등 35개는 16개 기관 중에 오직 하나에만 포함되어 있으며, 두 군데 이상 포함된 연구 주제로 많이 포함된 것부터 순서대로 나열하면 다음과 같다:

- 대응, 복구, 재구성(포렌식, 우아한 저하)(7군데 포함)
- 구조(결점 허용, 대규모 시스템을 위한 신뢰, 높은 보장)(6군데 포함)
- 모델링 및 시뮬레이션 도구(신뢰 특성용 포함)(5군데 포함)
- 진보된 개념/이론, 이론적 기초, 취약성 이론
- 탐지, 경보, 경고, 대응 개선
- 보안 관리 인프라(사고 관리 포함)(이상 4군데 포함)
- Best practices(SCADA 시스템을 위한 우아한 저하 포함)
- 위협의 특성화 및 통지
- 다른 조정 및 보안(국가적 ID, 전략적 통신 계획)
- 보호(예, 암호화, 침입 허용, 안전한 이동 코드 등)
- 네트워크 용 보안(고성능 암호화, 신뢰성)(이상 3군데 포함)
- 응용 보안(데이타 마이닝 포함)(이하 2군데 포함)
- 민감한 정보의 통제된 공유
- 탐지, 분석, 예방(센서 퓨전, 복잡한 공격)
- 대규모 데이터 시스템(추론/집합, 안전한 저장)
- 보안 메트릭스
- 조직 및 사회 차원
- 서비스 거부 공격 예방 및 저항
- 위험, 취약성
- 상황 인식(정책 및 키 관리, 사이버 패널)

여기서 다루어야 할 어려운 문제는 다음과 같다:

- 어젠다 비교를 용이하게 하고, R&D 커뮤니티 사이의 중복 어젠다 식별, 국가 R&D 어젠다 내의 갭 식별을 위한 공통 포맷, 용어, 시맨틱스
- 특정 R&D 도메인 내의 R&D 관심 분야의 초점을 맞추기 위한 구조

7.3 문제 공간

문제 공간은 지속적인 기술 진화를 통하여 역동적으로 변화하면서, 정교한 공격을 통하여 쉽게 붕괴되는 다중의 상호작용과 상호의존성을 가진 복잡한 것으로 특성화된다.

여기서 다루어야 할 과제들은 다음과 같다.

- 위협의 개선된 특성화와 통지
- 취약성 정도 이해
- 연속적인 공격과 연속적인 손상을 일으키는 상호의존성의 식별
- 정보보증(IA) 사양서, 분석, 합성(synthesis)을 위한 기본적인 기초 개발을 포함한 IA 이론의 진보된 개념
- 고-신뢰 인프라 설계 및 공학

- 모델링 및 시뮬레이션 도구
- 최소 필수 서비스의 식별
- 미국 내에서 개발된 중요 소프트웨어

7.4 제휴

각 영역 내, 특별히 R&D 커뮤니티 사이뿐만 아니라 정부와 민간 부문사이의 전례가 없는 제휴가 요구된다. 이것은 지적 자본을 모으고 정보 공유를 개선하며, 정부 요구사항을 상업용 솔루션과 통합하고, 필요한 솔루션을 제공하기 위한 기본적인 개념을 생성하기 위한 의도이다. 동반 관계는 국가 보안, 법 집행, 시민권, 상업 및 다른 민간 부분까지 걸친다.

여기서는 다음과 같은 문제가 도전과제이다.

- 개선된 국가적 조정
- 개선된 법적 및 법 집행 프로세스
- 법적 데이터 및 조정을 제공하기 위하여 잘 정의되고 개선된 프로세스
- 표준화 과정을 통한 시장에서의 개선된 정부 영향
- 시간 프레임 안에서 타당한 더욱 현실적인 기대치의 채용
- 시장 대응 실패에 대한 법적 대응
- 정보 접근과 비밀성의 균형

8. 맺음말

카네기 멜론대의 CERT 센터는 현재 컴퓨팅 환경에 영향을 주는 6 가지의 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

아울러 이 센터의 디렉터인 Richard Perthia는 민감한 데이터를 보호하면서 공격에 견딜 수 있는 네트워크를 만들 수 있는 시스템과 운용 기술에 대한 연구에서 장기간 관점 및 투자를 유지하는 것이 매우 중요하다고 지적하였다.

국내에서 발표된 최근 해킹 동향으로 해킹과 바이러스 기술의 통합화, 인프라 공격의 증대, 해킹 매체 및 목적의 다양화, 해킹 기술의 고도화 등이 있다. 아울러 정보 보호와 사이버 공격의 지평이 시스템에서 네트워크로 확대되는 경향이다. 이와 같은 추세에 따라 차세대 정보보호 기술로 시스템 및 네트워크 모니터링, TCP/IP 역추적과 포렌식의 중요성 증대가 예상되며, 통합 보안 기술도 지속적으로 발전될 것이다. 또한 신뢰 보안 기술이 확대되고, 유무선 통합 보안 기술 및 통신과 방송의 융합 보안 기술이 발전되어야 한다[4].

이러한 변화 추세에 따라, 본고에서는 미국의 I3P의 보고서 내용을 중심으로 미국의 정보인프라 보호를 위한 연구개발 방향과 기술에 대하여 기관별로 고찰하고 제시하였다. 본고가 향후 국내의 정보 인프라 보호 연구개발 방향 정립에 기여하였으면 하는 바램 이다.

참고 문헌

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

[2] 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.

[3] U.S. Department of Homeland Security, Protecting Cyberspace.

[4] 서동일, "최근 정보보호 기술 개발 동향 및 전망", 2003. 12.22 발표자료, 한국전자통신연구원.

[5] 심원태, "네트워크 보안기술 전망", 2003. 9.25 발표자료, 정보통신진흥원.

[6] 오승희, 남택용, 손승원, "네트워크 보안 기술 동향", 주간기술동향 통권 1116호, 2003.10.07.

[7] 이윤철, "정보보호 제품동향 및 세계시장 현황", 주간기술동향 통권 1108호, 2003.08.12.

[8] 이윤철, "전세계 정보보호 및 Business Continuity 시장동향", 주간기술동향 통권 1127호, 2003.12.23.

[9] 전용희, 장종수, 손승원, "미국의 정보인프라 보호 연구개발 동향 분석", 전자통신동향분석, 제 19권 제 4호, pp96-108, 2004년 8월, 한국전자통신연구원.

[10] 전자신문, 10면, 정보화 · 솔루션, 2004년 3월 19일.

[11] 전황수, "미 · 일의 정보보호대책과 우리에게 주는 시사점", 주간기술동향, 통권 1092호, 2003.04.22.

[12] 황성원, "국내 정보보호 현황과 발전방향", 정보통신논단, 정보통신연구진흥원.

[13] 미국정부의 정보보호 기술 R&D 동향, 한국전자통신연구원 네트워크보안구조연구팀, 2003. 9.23.

전 용 희

1971년 3월 ~ 1978년 2월 : 고려대학교 전기공학과

1985년 8월 ~ 1987년 8월 : 미국 플로리다공대 대학원 컴퓨터공학과

1987년 8월 ~ 1992년 12월 : 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사

1978년 1월~1978년 11월 : 삼성중공업(주)

1978년 11월 ~ 1985년 7월 : 한국전력기술(주)

1989년 1월 ~ 1989년 6월 : 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA

1989년 7월 ~ 1992년 9월 : 미국 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA

1992년 10월 ~ 1994년 2월 : 한국전자통신연구원 광대역통신망연구부 선임연구원

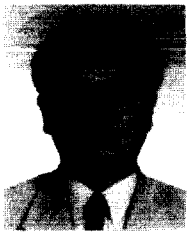
1994년 3월 ~ 현재 : 대구가톨릭대학교 컴퓨터·정보통신공학부 교수

2000년 1월 ~ 현재 : 한국통신학회 학회지 편집위원

2001년 3월 ~ 2003년 2월 : 대구가톨릭대학교 공과대학장 역임

2004년 2월 ~ 현재 : 한국전자통신연구원 정보보호연구단 초빙연구원

<관심분야> 네트워크 보안, 통신망 자원관리 및 성능분석, QoS 보장 기술



손 승 원

1984년 2월 : 경북대학교 전자공학과 공학사
1994년 2월 : 연세대학교 전자공학과 공학석사
1999년 2월 : 충북대학교 컴퓨터공학과 공학박사
1983년 8월 : 삼성전자(주) 연구원
1986년 4월 : LG 전자(주) 중앙연구소 H18mm 캠코더 팀장
1996년 12월 : 정보통신기술사 자격 취득
1991년 8월 ~ 2003년 12월 : 한국전자통신연구원 교환전송기술연구소 NTB 팀장, 인터넷 구조 팀장, 정보보호기술연구본부 정보보호응용연구부장, 동 네트워크보안연구부장 역임
2004년 1월 ~ 현재 : 한국전자통신연구원 정보보호연구단 단장/책임연구원

<관심분야> 정보보호, 네트워크 보안, Active Networks, Biometric Security