情 報 保 護 學 會 誌
第20卷 第1號, 2010. 2

정보 유출 방지 연구기술 동향

이 대 성*, 김 재 성**, 김 귀 남*

요 약

정보 기술의 발전과 격상된 국가 경쟁력으로 인하여 기업의 첨단 기술 보유 비율은 증가하고 있는 추세이며, 이로 인하여 기업의 핵심 기술 유출 피해도 꾸준히 증가하고 있는 실정이다. 산업 정보 유출은 한 기업뿐만 아니라 한 나라의 경제에 큰 피해를 주고 있기 때문에 국가차원에서 유출을 방지하기 위한 노력이 이루어져야 한다. 현재 산업 정보 유출을 방지하기 위해서 다양한 관련 법 재정과 여러 유관기관들의 연구가 진행되고 있다. 정보 유출 방지 연구는 크게 데이터 유출 방지 기술, 데이터 보호 기술, 사용자 인증 기술로 구분할 수 있다. 본 기고는 현재 국·내외 산업기술 보호 현황을 조사하고 정보 유출을 방지하기 위해 진행되고 있는 연구들을 간략히 소개하도록 한다.

Ⅰ. 서 론

정보통신 기술의 발전으로 인하여 기업에서부터 일반 개인에 이르기까지 정보기기 사용이 대중화되고 있으며, 우리 생활에 많은 부분을 차지하고 있다. 모든 기업의 업무와 정보는 전산기기를 통하여 이루어지고 있으며, 사용자에 대한 서비스 또한 많은 부분이 전산기기를 통해 이루어지고 있다.

이렇게 정보통신 기기의 대중화로 인하여 기업에서는 많은 산업 기밀 유출이 발생하게 되었고, 이로 인한 기업의 경제적 피해는 천문학적으로 늘어나고 있다[1-3].

최근의 IT(Information Technology) 보안 기술은 사이버 공간의 영역을 벗어나 물리 공간으로 확대되고 있으며, 이러한 추세를 반영하여 융합보안 기술에 대한 연구가 활발히 진행되고 있다. 또한, 산업간 융합, 기술간 융합화 추세에 따라 IT보안 기술과 물리보안 기술간의 융합을 통해 산업기밀 유출방지를 위한 새로운 연구개발에 대한 요구가 일어나고 있다.

기업이 기술을 개발하는 데는 많은 인력과 자금, 시간이 소요되지만, 산업스파이나 내부자에 의해 기술이 유출되는 데는 단 몇 분이면 충분하다. 막대한 자금과 인력을 투입하여 개발한 첨단기술이 보안관리 소홀로 인해 경쟁기업이나 해외로 유출된다면 해당 기업은 물론 국가 경쟁력에도 심각한 피해를 가져온다. 이에 기술 유출에 대응하는 기업들의 대응활동이 점차 늘어나고 노력하고 있음에도 불구하고, 기술 유출 사례는 더욱 급증하고 있다[2].

이를 예방하기 위해서 국·내외적으로 많은 연구가 진행되고 있으며, 크게 데이터 유출 방지 연구, 데이터 보호 기술 연구, 데이터 사용자 인증 기술 연구로 나눌 수 있다. 데이터 유출 방지 연구는 정보기기와 네트워크 기기에서의 데이터 유출을 탐지하고 예방하는 기술이다[6-11]. 데이터 보호 기술 연구는 데이터가 유출되어도 데이터에 대한 무결성, 기밀성, 안전성, 부인방지가 유지되도록 하는 연구이다[12-15]. 데이터 사용자 인증 기술 연구는 정보기기를 사용하는 사용자나 네트워크를 사용하는 사용자를 인증하는 기술로 물리적 인증을 비롯한 논리적 인증 체계를 연구하는 것이다[16-30].

본 기고는 최근 산업기술 유출 방지에 관한 국·내외 연구 동향과 장·단점에 대해서 살펴보고, 그 대응 기술에 있어 데이터 유출 방지 기술, 데이터 보호 기술, 사용자 인증 기술로 나누어 살펴본다.

구성은 다음과 같다. 제2장에서는 산업기술 유출 동향과 피해 사례를 분류하고 분석한다. 제3장에서는 데이터 유출 방지 기술에 대해서 살펴보며, 제4장에서는 데이터 보호 기술에 대해서 살펴본다. 제5장에서는 사

* 경기대학교 산업보안학과
** 한국인터넷진흥원 인터넷정보보호본부 공공정보보호단 지식정보보안산업팀

용자 인증 기술에 대해서 살펴보고, 제6장에서 결론을 맺는다.

Ⅱ. 국·내외 산업기술 보호

2.1 국내 산업기술 보호 현황

2.1.1 국내 산업기술 유출 피해

국내의 경우 국가경쟁력이 높아짐에 따라 불법적인 산업기술 해외 유출이 증가하고 있는 추세이다. [표 1]은 산업기술 해외유출 건수를 나타낸 것으로 2004년부터 2008년간 적발된 기술유출 시도는 총 160건으로, 유출되었을 경우 예상되는 피해액은 253.5조원으로 추정된다[1,2].

〔표 1〕 산업기술 해외유출 (적발 기준)

방지기술	2004	2005	2006	2007	2008	계
건수	26	29	31	32	42	160
피해예방액 (조원)	32.9	35.5	13.6	91.7	79.8	253.5

유출 피해 동향을 보면 과거에는 한국이 강세를 보이는 반도체·휴대폰 등 IT분야에 기술 유출이 집중되었으나, 최근 들어 정밀기계, 화학 등 전 분야로 확산되고 있다[2].

2.1.2 국내 산업기술 보호

국내 산업기술 보호는 1987년 부정경쟁 방지 및 영업비밀 보호에 관한 법률이 재정되면서 본격적으로 시작되었다. 또한, 사업 기술 유출을 방지하기 위해서 2006년 10월 "산업기술의 유출방지 및 보호에 관한 법률" (이하 산업기술유출방지법)을 마련하여 산업기밀 해외 유출을 차단할 수 있도록 법적 재정이 마련되었으며, 정부는 2003년 국가정보원에 산업기밀보호센터를 설립하여 해외 산업기밀 유출을 예방하고 있다.

국내 산업기술 보호에 관한 연구는 일부 산·학·연에서 소규모로 진행되어 오다가 2008년 6월 지식경제부 지정 지역혁신센터(RIC)로 선정된 산업기술보호특화센터가 설립되어 본격적인 산업기술 보호 연구가 진행되고 있다. 또한, 기존의 산업기술보호협회를 비롯한 경기산업기술보안협의회가 추가로 설립됨에 따라 산업기술 보호에 대한 인식 제고와 더불어 산·학·연 및 지역별 협력이 진행되고 있다.

2.2 해외 산업기술 보호 현황

2.2.1 미국의 산업기술 보호

미국의 경우 산업기술보호 추진체계는 통일영업비밀보호법(UTSA: Uniform Trade Secrets Act), 경제스파이법, EXON-FLORIO조항, 방첩활동강화법, TAL (Technology Alert List), 수출관리규정(Export Administration Regulation, EAR) 의 대표적인 6가지 법안을 이용해서 보호하고 있다. 미국은 정부 차원의 관련 법률 정비와 처벌 강화 및 이를 통한 기술유출 예방을 목표로 하고 있으며, 정보수사기관의 인력 확충 및 조직 강화에 주력하고 있다.

또한, 미국은 국방부에서부터 국무부에 이르기까지 첨단 기술 유출을 방지하기 위한 유기적 공조 시스템 구축을 진행하고 있다[4].

2.2.2 일본의 산업기술 보호

일본은 부정경쟁방지법을 기본으로 하여 '기술유출 방지 지침', '영업비밀관리지침'을 이용하고 있으며, '기술거래 및 공동 연구에 대한 지침'을 통하여 산업 기술 유출 예방에 매진하고 있다[5].

일본은 다른 나라와 다르게 민간의 자율적 산업기술 보호를 유도하고 있으며, 외국의 자국내 산업기술 습득에 제한을 두어 산업기술 유출의 원천봉쇄를 유도 하고 있다.

2.2.3 중국의 산업기술 보호

중국의 경우 산업기술 유출을 국가안보의 위해행위로 판단하여 위반 시 법정최고형까지 처벌이 가능하도록 강력한 처벌규정을 통하여 산업기술 유출을 방지하고 있다.

중국은 "기술 수출입 관리 조례"를 통하여 수출 대상 기술을 수출자유, 제한기술, 금지기술로 구분하여 엄격

하게 관리하고 있으며, '인터넷관련 기밀보호법'(2000년)으로 인터넷을 통한 첨단 기술 및 국가 기밀의 유출 행위를 금지하고 국가 비밀기술의 수출 시에는 국가과학기술위원회의 허가를 받도록 규정하고 있다[5].

Ⅲ. 데이터 유출 방지 기술

3.1 데이터 유출 방지 기술 요소

데이터 유출 방지 기술, 즉 DLP(Data Loss Preventrion)는 기업 구성원, 프로세스, 기술의 결합을 통해 고객 혹은 직원의 기록 등 개인정보, 기업정보, 제품 계획, 소스코드와 같은 지적 재산을 포함하는 기밀정보 등이 기업 밖으로 유출되는 것을 방지하는 연구이다. 초기 DLP는 주로 고객정보를 대량으로 다루는 금융 및 보험 산업 분야에서 도입되어 사용되었지만 최근 대규모 개인정보 유출사고를 비롯해 산업기술 유출 사고가 심각해지고 있는 상황으로 정보유출 방지가 모든 산업에서 중요한 요소로 인식되면서 DLP에 대한 관심과 요구가 끊임없이 증가하고 있다. DLP 기술은 [표 2]와 같이 크게 4가지로 구성할 수 있으며 각 요소는 다음과 같다[6].

〔표 2〕 정보유출 방지 기술 요소들의 장·단점

방지기술	장점	단점
접근제어	사용자별, 파일별, 세부적 제어가능	관리 작업이 많고 정적인 관리
암호화	인증 받지 못한 사용자는 접근불가	관리 작업이 많고 정적인 관리
필터링	정해진 규칙에 대한 높은 효율	기업/기관 특성에 따라 정확도 차이남
활동감시	기밀유출에 대한 탐지기능 제공	오탐 가능성이 있고 실시간 차단 아님

3.1.1 접근제어

접근제어는 사용자별, 파일별 등 세부적으로 제어가 가능한 기밀 유출 방지 기법이다. 정보의 내용 및 중요도에 따라 정보를 그룹화하고, 각 정보에 대한 접근권한을 관리 하는 것으로 시스템 접근제어와 물리적 접근제어로 나누어 볼 수 있다. 시스템 접근제어는 각 중요정보에 대해 직급, 직위, 즉 사용자 역할별 접근제어 기능을 제공하는 것으로 DLP에서는 일반적으로 기업 내 인사관리 DB와 연결하여 역할기반 접근제어(Rule Based Access Control: RBAC)를 수행하는 기능을 가지고 있다. 또한 접근제어의 기능 안전성을 위해 최근에는 가상화 기술을 접목하여 접근이 허락된 인가자만가상 저장소에 정보를 저장하는 등 안전성을 제공하는 기술이 개발되고 있다. 한편 DLP에서 제공하는 물리적 접근제어, 일반적으로 매체제어를 의미하는 것으로 특정 시스템에 대한 USB, CD 등 정보 유출이 가능한 보조기억매체의 접근은 인가된 내부자만이 수행할 수 있도록 하는 기밀유출 방지 기법이 있다.

3.1.2 암호화

데이터 유출 방지 기술, 즉 DLP에서는 내부 정보에 대한 외부의 불법침입 및 송수신 상의 정보 유출 등을 방지하기 위해 암호화 기술을 제공하고 있다. 일반적으로 암호화 기술은 접근제어 기술과 결합하여 사용되어진다. 형태는 DRM과 유사하며 자체적으로 암호화 기능을 제공하기 보다는 DRM 등과 연계하여 상호보완적인 역할로 적용되고 있다. 암호화는 정보보호 측면에서 높은 효율을 보이지만, 키의 안전한 관리 및 분배, 키 분실 시 복구 등에 따른 불편함, 암호화된 정보의 효과적인 검색 문제 등이 단점으로 지적된다.

3.1.3 필터링

필터링은 내부에서 외부로 반출되는 트래픽, 정보 등에 대해 일정 규칙에 따른 검사 후 이를 제어하는 기술을 의미한다. DLP에서 필터링은 트래픽 제어, 콘텐츠 제어 등으로 나누어지는데, 트래픽 제어는 프로토콜 및 서비스에 따라 이용을 제한하는 것으로, 예를 들면 FTP, 메신저, P2P, 웹메일 등의 유출 가능성 있는 서비스 이용을 제한하는 것을 의미 한다. 또한 콘텐츠 제어는 여러 가지 경로로 외부에 송신되는 정보에 대해 자동 검사 후 발송 여부를 판단하는 기능을 의미한다. 필터링 기술에서 현재 트래픽 제어는 문제없이 수행되고 있으나, 콘텐츠 제어기술은 콘텐츠 별로 중요도를 판단하는 기준이 각 기업 및 기관의 특성에 따라 달라서 정확도가 상당히 낮은 것이 단점이다.

3.1.4 활동감시

활동감시 데이터 유출 방지 기술은 정보 유출에 대한 분석 및 추적을 수행하기 위해 내부에서 진행되는 유출 가능성 있는 모든 프로세스 감시 및 이력 관리를 통한 정보 유출 탐지 업무를 수행하는 방지 기술을 말한다. 이는 회사의 내부 규정 및 법규를 기반으로 보안정책을 관리하며, 외부에 송신되는 정보는 아카이빙 기반으로 모두 로깅되어 사후 분석에 활용된다. 이 기법은 활동 관련 모든 정보가 로깅된다는 측면에서 각 내부자에게 경각심을 주는 등 사전 방지효과가 크나, 실제 감시 프로세스가 정보유출이 발생한 사후에 이루어져서 사전 방지가 이루어지지 못하고, 유출 발생 후 이에 대한 조치를 해야 한다는 것이 단점이다. 또한 사후 분석을 하기 위해서는 많은 시간이 투입되고, 시간을 절감하기 위한 자동 분석은 정확도가 떨어지는 점도 문제점으로 지적되고 있다.

3.2. 데이터 유출 방지 제품[7]

3.2.1 SCM(Secure Content Management)

SCM[8]은 IDC에서 정의한 용어로서 웹, 이메일 및 인터넷 응용 프로그램을 통해 내부 망에 유입/출입되는 비정상 콘텐츠에 대한 바이러스 차단, 스파이웨어 차단, 웹 필터링, 메시징 보안 등의 4대 보안 기능을 포함하고 있는 통합 콘텐츠 보안 제품이다. 이중 메시징 보안은 e-mail, IM, SMS 그리고 P2P를 통하여 유포되는 스팸 및 성인 콘텐츠를 필터링하는 기능뿐만 아니라, 내부 기밀정보의 유출을 탐지하고 차단하는 기능을 포함한다.

3.2.2 OCC(Outbound Content Compliance)

OCC[9] 역시 최근 조직내부의 보안 위협에 대한 관심의 증가로 새롭게 형성되고 있는 보안 솔루션이다. 이메일, IM, P2P, FTP, 웹 포스팅 그리고 이외의 메시징 트래픽에 포함되어 내부로부터 유출되는 콘텐츠를 감시하고, 암호화, 필터링 및 차단 기능을 제공하며 공기관과 산업체의 내부 규정(HIPAA, GLBA, SOX 등) 위반, 조직 내부의 이메일 정책이나 관행 위반, 지적재산권 유출, 기밀정보 유출, 성인 콘텐츠 유포 등에 대한 방어 기능을 포함한다. OCC는 크게 5분야로 나누어지며, 이는 email filtering, secure email(encryption), multiprotocol content filtering, instant messaging security, ERM 등과 같다. 그중 multi-protocol content filtering 분야는 기존의 전통적인 이메일 보안을 넘어서 다양한 프로토콜을 통하여 전달되는 메시징 트래픽을 모니터링하여 조직내부의 중요 정보유출을 차단하는 기능을 제공함으로서 향후 내부 기밀정보 유출방지 솔루션으로 각광받고 있다.

3.2.3 ILD&P(Information Leackage Detection and Prevention)

ILD&P[10]는 내부의 민감 정보의 불법 유출을 최소화하기 위하여 최근에 등장한 보안 솔루션을 포함한다. ILD&P 시장이 성장할 수 있는 동인은 법적인 동인과 기술적인 동인이 있다. 법적인 동인은 European Union Data Protection Directive, Basel II Accord, Sarbanes-Oxley Act of 2002(SOX), HIPAA(Health Insurance Portability and Accountability Act), Gramm-Leach Bliley Act(GLBA), California SB 1386, 일본의 개인정보 보호 법안 등이 있다. 기술적인 동인은 기업 환경에서 인스턴스 메신저와 P2P 프로그램과 같은 네트워크 응용 프로그램의 증가에 따른 기밀 유출 가능성의 확대와 정보 유출 사고의 증가 등이다.

3.2.4 CMF(Content Monitoring and Filtering)

가트너에서 정의한 용어로서 내부망에 유출입되는 트래픽의 패킷을 캡처링하고 세션관리를 통하여 언어기반으로 내용을 분석함으로써, 사전에 정의된 룰이나 정책에 의해 기밀정보의 유출을 탐지 및 차단하는 기능을 제공한다. CMF 시장은 2001년부터 있었으나 대부분의 업체는 시장에 진입한지 2년 이내의 신생업체들이다[11]. CMF 제품의 진정한 가치는 기업이나 기관의 관리자가 잘못된 비즈니즈 프로세스나 정보 유출 취약 지점을 사전에 발견하고 조치를 취할 수 있게 도와주는데 있다.

Ⅳ. 데이터 보호 기술

4.1 데이터 보호 기술 요소

DRM(Digital Rights Management)이란 디지털 콘텐츠의 불법 유통과 복제를 방지하고, 적법한 사용자만이

데이터를 사용하게 하며, 저작권자의 권리 및 이익을 보호하는 시스템을 의미한다.

DRM 기술은 크게 사용자 허가와 데이터 유출 추적 기술로 나눌 수 있다. 사용자 허가 기술은 데이터를 정당한 권리를 가진 사용자에게만 안전하게 전송하고 허가된 사용범위 내에서 사용하게 제한하는 방법이다[12]. 데이터 유출 추적 기술은 불법적인 방법으로 데이터가 복제되고 유출될 경우, 해당 데이터의 저작권자가 누구인지 증명하고 어떤 경로를 통하여 불법 복제되고 유출되었는지를 추적하는 기능이다[13].

데이터 보호 기술은 기본적으로 지속적 보호, 편리성, 유연성, 불법 사용 방지, 용이성 등의 5가지로 나눌 수 있으며, 각 요소의 내용은 다음과 같다.

4.1.1 지속적 보호

데이터 사용 과정의 무결성과 비밀성 보장, 데이터를 관리하는 DRM 에이전트의 외부공격에 대한 강인성이 보장되어야 한다. 또한 데이터는 한번 암호화된 후에 계속 암호화된 상태로 존재하고 소유자의 저작권 통제를 받기 때문에 원본 데이터가 유출될 여지가 없다. 저작권 권한을 받은 사용자라 하더라도 원본을 추출하여 다른 용도로 사용할 수 없도록 지속적인 보호가 가능해야 한다.

4.1.2 편리성

데이터의 저작권 보호를 위해 사용자에게 불편을 초래하지 않도록 편리성이 제공되어야 한다. 사용의 편리성을 제공하기 위해선 사용자가 데이터를 쉽게 검색하고 사용할 수 있어야 하며, 허가된 권리 내에서 자유롭게 데이터를 사용하는 것을 보장해야 한다.

4.1.3 유연성

여러 종류의 데이터 형식을 지원해야 하고, DRM 간의 연동 오류에 따른 피해를 최소화해야 한다. 유연성에는 문서, 멀티미디어 콘텐츠, 웹 기반의 콘텐츠, 소프트웨어 그 밖의 디지털 데이터 등 다양한 데이터 형식을 지원해야 한다. 또한 DRM 시스템의 상이함으로 인해 발생하는 사용자의 권리 제한의 문제 해결이 보장되어야 한다.

4.1.4 불법 사용 방지

데이터의 물리적인 복제는 무한히 허용되나, 실제 복제된 데이터의 사용은 합법적인 권한을 발급받지 않는 한 허용하지 않도록 해야 한다. 이로 인해 데이터의 불법 사용 및 불법 복제를 강력하게 제어할 수 있다.

4.1.5 용이성

데이터에 대한 수신자가 또 다른 임의의 수신자에게, 다시 그 수신자는 또 다른 제3의 수신자에게 암호화된 데이터를 전달하고 사용할 수 있도록 할 수 있어 한다. 안전하게 암호화된 데이터 공유에 있어서 어떠한 제약이 따르지 않아야 한다.

4.2 데이터 보호 기술 제품

4.2.1 파수닷컴 社

파수닷컴社 제품으로는 크게 3가지로 Enterprise DRM 및 Consumer DRM, Personal DRM으로 분류할 수 있다. 이중 EnterpriseDRM은 AES, RSA 등 암호 알고리즘을 사용하여 문서를 암호화하고 문서의 사용기간/횟수 및 사용 PC 대수 등 다양한 보안 정책 설정 및 제품별로 관리하던 정책/인증/감사/모니터링 기능을 하나의 프레임워크에서 통합관리하는 시스템이다[13].

4.2.2 마크애니 社

마크애니社는 대표적인 제품 중 문서보안 제품인 Document Safer와 워터마킹 제품인 MAIM으로 분류 할 수 있다. Document Safer제품은 국제공인 암호화 방식에 의한 패키징 시스템이고 DB파일 암호화, MDI기능을 제공하고 MAIM 제품은 삽입 모듈과 검출 모듈은 각각 따로 제공되며 검출모듈에 워터마크의 존재를 판별하는 기능이 포함되어 있다. 마크애니社는 다수의 특허기술을 보유하고 있으며 해외 시장 진입을 활발히 진행 중이다[14].

4.2.3 소프트캠프 社

소프트캠프社의 제품 중 문서보안 제품인 SoftCamp

Document Security는 조직의 중요 문서에 대해 사용자 권한과 정책을 설정해 전자문서나 인쇄물에 대해 보안성을 높이며, 로그정보를 통해 사전 예방 및 사후 감사를 가능하게 하는 내부 정보 유출 방지 솔루션이다. 이는 조직 내 정보공유시스템에 축적된 핵심 정보 및 직원 PC에 저장된 중요 문서, 업무를 통해 생성하는 모든 문서에 대해 강력한 보안을 제공하고, 안전하게 유통할 수 있도록, 통합적이고 전사적인 보안 정책을 기반으로 문서의 생성 및 유통, 보관, 반출에 이르기까지 보호 및 관리를 체계적으로 지원한다[15].

V. 사용자 인증 기술

산업기술 보호 연구에서 가장 오래도록 연구되어 온 것이 사용자 인증 기술이다. 사용자 인증 기술은 물리적 인증 기술과 논리적 인증 기술로 나눌 수 있으며, 인증 기술은 사용자 바이오 정보를 이용한 물리적 인증을 비롯하여 네트워크 데이터 패킷의 인증에 이르기까지 매우 다양하다.

대표적인 물리적 인증 기술은 사람의 바이오 정보를 이용한 바이오 인증 기술[16-28]과 RFID와 같은 센서를 이용한 센서인증 기술[29-30]이 있다.

5.1 물리적 인증 기술

본 기고에서는 현재 바이오 정보를 이용한 인증기술 중 지문인식 기술과 얼굴인식 기술의 연구에 대해서 살펴보겠다.

5.1.1 지문인식을 이용한 사용자 인증

지문인식을 이용한 사용자 인증은 가장 고전적이면서 현재까지 많이 사용되고 있는 방식이다. 지문인증 방식은 비밀번호에 해당하는 데이터베이스 내의 사용자 지문 정보만을 비교하여 판단하는 자동 지문 검증 방식과 사용자의 지문을 데이터베이스에 저장된 지문정보와 비교하여 일치하는 데이터를 찾는 자동 지문 인증 방식으로 나눌 수 있다[16-23].

지문인식 연구는 크게 특징점 추출과 지문 정합으로 나눌 수 있는데, 특징점 추출은 지문을 대표할 수 있는 값들을 추출하는 것이며, 지문 정합은 비교하는 두 지문 간의 특징점 분포의 유사성을 검사하고 이를 일정 범위의 점수로 나타내는 것이다. [표 3]은 특징 추출관련 연구를 나타낸 것이며, [표 4]은 지문 정합관련 연구를 나타낸 것이다.

〔표 3〕 특징 추출 관련 연구

구분	제안 알고리즘
방향행렬 알고리즘[16]	지문 구조를 표현할 수 있는 방향 행렬(direction matrix)을 생성하여 이렇게 얻은 방향성 지도로부터 코어와 델타를 찾아냄
Gabor 필터 알고리즘[18]	전처리 과정없이 Gabor 필터를 사용하여 코어를 찾아내고, Gabor 특징을 이용한 정합 방식을 제안함
회색 음영 특징점 추출 알고리즘[18]	이진화, 세션화 과정 없이 회색 음영 이미지에서 융선을 따라가며 특징점을 추출함
이미지 에너지 분서를 이용한 알고리즘[19]	서로 다른 크기와 방향에 대한 이미지의 에너지 분포(energy distribution)의 근사값으로 표현되는 특징 벡터를 정의하고, 교차 연산자를 사용하여 특징 벡터들 간의 유사성을 측정함

〔표 4〕 지문 정합관련 연구

구분	제안 알고리즘
스트링 정합 알고리즘[21]	스트링 정합 알고리즘을 사용하여 입력된 이미지와 등록된 템플릿 간의 대응 특징점을 찾는 검색과정을 최소화하고, 지문 간의 위치 변환과 비선형 변형 문제를 극복하기 위한 정렬 기반 정합 알고리즘
경량화된 정합 알고리즘[22]	제한된 하드웨어 환경(스마트카드)에서 수행속도를 감안한 효과적인 정합 수행 방식을 제안함
moving window 정합 알고리즘[22]	움직임 창(moving window)을 이용하여 처리속도와 안전성을 개선함
bounding box 정합 알고리즘[23]	스트링 정합 알고리즘을 수정하여 개선시킨 것으로, 크기가 변하는 오차 허용 영역(bounding box)을 사용함

5.1.2 얼굴인식을 이용한 사용자 인증

얼굴 인식은 크게 정지영상을 이용한 얼굴 인식과 동영상을 이용한 얼굴 인식이 있다. 정지영상을 이용한 얼굴인식 연구에는 추출된 얼굴영상을 통계적 방법을 이용하여 인식하는 방법[24], 신경망 알고리즘을 이용한 방법[25], 2차원 측면 영상을 사용하여 인증하는 방법[26], 3

차원 영상을 사용하는 방법 등이 있다[26].

동영상을 이용한 얼굴 인식은 움직이는 영상에서 사람의 영상을 분리하여 특징점을 추출하는 방법과 얼굴의 3차원 모델을 모델 기반의 압축 연구[27]가 있다. 현재 얼굴인식분야의 연구는 다양한 표정을 가지는 얼굴을 이식할 수 있는 얼굴 표정 인식과 인증 기술이 활발이 연구되고 있다[28].

5.1.3 센서정보를 이용한 사용자 인증

센서정보를 이용한 사용자 인증은 현재 RFID를 이용한 인증방식이 많이 연구되어 사용되고 있다. RFID는 리더를 소유한 사람과 물리적 접속 없이 태그의 정보를 읽기 때문에 간편하다는 장점이 있다.

RFID를 이용한 연구는 인증 프로토콜을 개선하는 방법으로 연구가 집중되고 있으며, 대표적으로 해쉬 락(Hash lock)을 이용한 방식[29], 확장된 해쉬 락을 이용한 방식[30], 해쉬 체인을 이용한 방식[30]등이 있다.

센서정보를 이용한 인증은 RFID정보를 휴대하고 간편하게 인증할 수 있다는 장점이 있지만, 대체 인증이 가능하다는 단점이 있다.

5.1 논리적 인증 기술

논리적 인증 기술은 물리적 공간에서의 인증이 아닌 사용자가 사용하고 있는 정보에 대한 인증을 말한다. 이는 단순한 사용자 인증을 넘어선 사용자가 다른 사용자와 송·수신하는 정보에 있어서 데이터를 인증하는 기술을 말한다. 논리적 인증 기술은 크게 암호 기술을 이용한 인증 기술과 바이오 정보를 이용한 인증 기술로 나눌 수 있다.

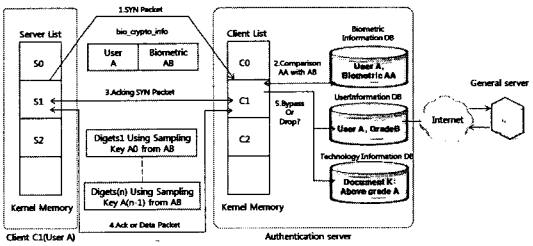
5.1.1 암호기술을 이용한 논리적 인증

가장 대중화되고 활발하게 연구되고 있는 분야로 다양한 암호 알고리즘과 프로토콜을 이용하여 사용자를 논리적으로 인증하고 있다. 이러한 인증 방법은 암호키가 노출될 경우 대체 인증이 가능하다는 단점이 있으며, 실제 사용자가 사용하고 있는지는 완벽하게 알 수 없다는 단점이 있다.

5.1.2 바이오 정보를 이용한 논리적 인증

현재 일부 연구 기관에서 바이오 정보를 이용한 논리적 인증이 연구되고 있다. 가장 활발히 연구되고 있는 것이 네트워크 패킷 데이터에 바이오 정보를 삽입하여 패킷을 보내는 사람이 누구인지를 인증하는 방식이다.

[그림 1]은 네트워크 패킷 데이터에 바이오 인증 정보를 삽입하고 인증하는 시스템 구조를 나타낸 것이다.



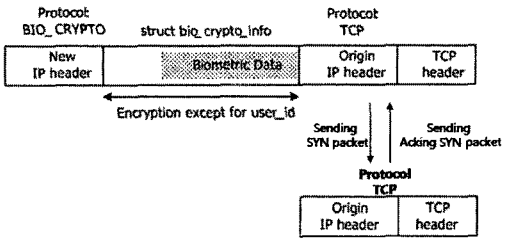
〔그림 1〕 바이오 정보를 이용한 네트워크 패킷 인증

[그림 1]의 1단계는 클라이언트가 일반서버로 전송하는 SYN 패킷을 중간 인증서버에서 들여다보는 과정을 보여준다. 이때 전송되는 SYN 패킷은 일반적인 TCP SYN 패킷과 다르다. 전송되는 SYN 패킷은 사용자 A의 암호화된 바이오정보(AB)를 포함하고 있다.

[그림 1]의 2단계는 실시간으로 수집되어 전송된 바이오 정보(AB)를 데이터베이스에 등록되어 있는 바이오 정보(AA, 사용자가 현장 방문하여 등록한 바이오 정보)와 비교하여 인증한다. 이때, 비교되는 두 바이오 정보(AA, AB)가 100% 일치하거나 일정 경계(threshold) 값을 만족시키지 못하면 인증에 실패한다. 실시간으로 수집되어 전송된 바이오정보는 바이오정보의 특성상 데이터베이스에 저장되어 있는 바이오 정보와 100% 일치하는 것이 거의 불가능하기 때문에, 이 경우는 복사본으로 간주하고 실패 처리한다.

인증이 성공하면 클라이언트(C1)에 관한 정보(바이오정보, IP주소, 포트번호 등)는 인증서버의 Client List 자료 구조 형태로 커널 메모리에 현재 세션 기간 동안 유지되고, 바이오정보를 포함했던 패킷은 [그림 2]와 같이 중간 인증서버에서 변형되어 외부로 전송된다.

[그림 1]의 3단계는 TCP/IP 3-방향 핸드쉐이크 프로토콜 과정에서 일반서버가 보내는 Acking SYN 패킷을 중간 인증서버에서 [그림 3]과 같이 바이오정보가 포함



〔그림 2〕 인증서버에서 변조되는 패킷 변화

된 패킷 형태로 변조하여 보내게 된다. 중간 인증 서버가 보내는 Acking SYN 패킷도 일반적인 TCP Acking SYN 패킷과 다르다. 이때 보내는 Acking SYN 패킷은 향후 통신에 있어 HMAC[7] 해쉬 계산을 위한 암호키를 바이오정보로부터 어떻게 추출할 것인지에 대한 지시 사항을 포함하고 있다. 이러한 지시 사항은 클라이언트가 [그림 1]의 1단계에서 보냈던 SYN 패킷처럼 bio_crypto_info 구조체 내에 포함된 형태로 일회성 세션키를 통해 암호화되어 전송된다.

클라이언트는 SYN 패킷 전송 시에 실시간으로 수집된 바이오 정보([그림 2]의 회색 영역)와 추가적인 정보(바이오정보의 크기, 시퀀스 번호 등)를 bio_crypto_info 구조체에 포함시킨 후 사용자 ID를 제외하고 bio_crypto_info 구조체를 일회성 세션키로 암호화하여 전송한다.

중간 인증서버가 Acking SYN 패킷을 전송 시에도 bio_crypto_info 구조체 형태로 암호화되어 전송되며, 이 때는 향후 통신에 있어 클라이언트가 바이오정보로부터 HMAC 해쉬 암호키를 어떻게 추출할 것인지 알려주는 지시를 담고 있다.

[그림 1]의 4단계에서는 클라이언트가 마지막 ACK 패킷을 전송함으로써 TCP 3-방향 핸드쉐이크를 완성한다. 이때부터 [그림 1]의 3단계에서 서버가 알려준 지시에 따라 난수를 생성하고 바이오정보 중에서 생성된 난수로부터 56 비트(bit) 영역을 추출하고 이 영역을 바이오패킷의 HMAC 해쉬 계산용 암호키로 사용한다.

[그림 1]의 5단계는 TCP 3-방향 핸드쉐이크 완성 후, 데이터 통신 시에 데이터의 정보 등급과 사용자별 권한 등급을 비교하여 패킷 차단여부를 결정하는 과정이다. 사용자 권한등급보다 데이터 정보등급이 높은 경우는 패킷을 차단하여 외부로 유출되지 않도록 한다.

V. 결 론

지식정보사회에서 가장 중요한 것은 기업이 갖고 있는 정보 및 지적 재산권 등 그간 쌓아온 기술들일 것이다. 따라서 산업기술 유출방지의 피해를 최소화 하는 연구가 향후에도 활발히 진행될 것으로 기대된다.

기업보안 정보유출 방지기술은 개인 PC, 네트워크, 물리적 보안 등 이상행위를 탐지하기 위한 유형, 무형의 보안 장치가 필요하다. 이들 중에는 정보유출 방지 기술인 DLP, 데이터 보호 기술인 DRM, 바이오 정보를 이용한 사용자 인증 등 내부 유출을 막고 외부로부터 위협을 보호하는 기술들이 현재 활발히 연구 중이고 실무에서도 널리 활용되고 있다.

기업이 보안 관리를 하는 목적은 기업의 존립이나 영리, 명예를 관리하는데 있다. 기업이 보안 관리해야 할 대상, 즉 보안의 객체는 기업이익에 반하는 모든 것으로 생각할 수 있다. 본 기고에서 제시하는 기술들은 기업보안 정보유출 방지를 최소화 하는 일례의 기술들이다.

참고문헌

[1] 산업기밀보호센터, "첨단 산업기술 보호동향 9호" pp. 65-99, 2008.

[2] 노호래, "산업기술 유출범죄에 대한 정책적 대응방지", 한국공안행정학회, 2008.

[3] 산업보안연구학회 논문지(vol.1, no.1), "기술 유출이 산업에 미치는 피해 추정기법에 관한 고찰", 2008.

[4] 김민배, "국가핵심기술 기준과 국가안전보장", July, 2008.

[5] 임영모, 박성배, 최병삼, "핵심기술 해외유출의 실태와 대책", CEO Information, October, 2008.

[6] 남기효, 강형석, 길지호, 김성인, "내부정보 유출방지(DLP) 기술동향" 정보통신산업진흥원, September 9, 2009.

[7] 이호균, 이승민, 남택용, 장종수, "기밀정보 유출방지 기술 동향" 정보통신산업진흥원, July 26, 2006.

[8] Brian E. Bruke, Rose Ryan, "Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc,"

IDC, Nov, 2005.

[9] Brian E. Burke, "Worldwide Outbound Content Compliance 2005-2009 Forecast and Analysis: IT Security Turns Inside Out," IDC, Nov, 2005.

[10] Dan Yachin, "InfoWatch: A Multilayerd Approach for Information Leakage Detection and Prevention," IDC, September, 2005.

[11] Raul E. Proctor, Rich Mogull, "Magic Quadrant for Content Monitoring and Filtering," Gartner, February 17, 2006.

[12] 최종현, 이병희, 김승주, 원동호, "DRM(Digital Rights Management)기술", 정보과학회지 제25권 제5호, 2007. 5, pp. 17~21.

[13] http://www.fasoo.com.

[14] http://www.markany.com/.

[15] http://www.softcamp.co.kr/.

[16] C. Hsieh, Z. Lu and T. Li, K. Mei, "An Effective Method to Extract Fingerprint Singular Point", *Proc. of 4th International Conference/ Exhibition on High Performance Computing in the Asia-Pacific Region*, 2000, pp. 696-699.

[17] C. Lee and S. Wang, "A Gabor Filter-based Approach to Fingerprint Recognition", *IEEE Workshop on Signal Processing Systems*, 1999, pp. 371-378.

[18] D. Maio and D. Maltoni, "Direct Gray-scale Minutiae Detection in Fingerprints", *IEEE Trans. on PAMI*, Vol. 19, 1997, pp. 27-40.

[19] M. Tico, P. Kuosmanen, and J. Saarinen, "Wavelet Domain Features for Fingerprint Recognition", *Electronics Letters*, 2001.

[20] N. Ratha, K. Karu and S. Chen, A. Jain, "A Real Time Matching System for Large Fingerprint Databases", *IEEE Trans. on PAMI, Vol.* 18, 1996.

[21] Y. Moon, H. Ho, S. Wan, and S. Wong, "Collaborative Fingerprint Authentication by Smart Card and a Trusted Host", *Proc. Canadian Conference on Electrical and Computer engineering*, 2000.

[22] H. Yahagi, S. Igaki, and F. Yamagishi, "Moving window Algorithm for Fast Fingerprint Verification", *Proc. of the IEEE Southeastcon'90*, 1990, pp. 343-348.

[23] X. Luo, J. Tian, and Y. Wu, "A Minutia Matching Algorithm in Fingerprint Verification", *Proc. of 15th International Conference on Pattern Recognition*, 2000.

[24] 이철한, 정민이, 김종선, 최정윤, 김재희, "통계적 형상 기반의 얼굴인식을 위한 가변얼굴템플릿 생성 방법", *대한전자공학회*, 전자공학회논문지-SP, 電子工學會論文誌 第44卷 SP編 第2號, 2007. 3, pp. 27~36.

[25] 양욱일, 손광훈, "방사 기저 함수 신경망을 이용한 3차원 얼굴인식", *대한전자공학회*, 전자공학회논문지-SP, 電子工學會論文誌 第44卷 SP編 第2號, 2007. 3, pp. 82~92.

[26] F. Pighin, J. Hecker, D. Lischinski, R. Szeliski, and D. H. Salesin, *Syhthesizing realistic facial expressions from photographs. In computer Graphics SIGGRAPH'98 Proceedings*, 1998, 231-242.

[27] 이호근, 정성태, "빠른 얼굴 검출을 이용한 실시간 얼굴 인식 시스템", *한국정보과학회*, 정보과학회 논문지 소프트웨어 및 응용 제32권 제12호, 2005. 12, pp. 1247~1260.

[28] 양희성, 김유호, 이준호, "조명 변화, 얼굴 표정 변화에 강인한 얼굴 인식 방법", *한국정보과학회*, 정보과학회논문지 소프트웨어 및 응용 제28권 제2호, 2001. 2, pp. 192~200.

[29] S. A. Weis(2003), "Radio-frequency identification security and privacy", *Master's thesis, M.I.T*, 2003.

[30] S. A. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy aspects of low-cost radio frequency identification systems", In First International Confeence on Security in Pervasive Computing, LNCS 2802, pp.201-212, Springer-Verlag, 2003.

[31] 김재성, "바이오인식과 산업기술보호", 한국인터넷정보학회 춘계학술대회, 2009. 5. 22.

〈著者紹介〉

이 대 성 (Daesung Lee)
정회원
1992년 2월: 인하대학교 전자계산공학과 졸업(학사)
2001년 2월: 인하대학교 전자전자계산공학 졸업(석사)
2005년 6월~2007년 11월: 아인픽춰스 VR 연구소 선임연구원
2008년 2월: 인하대학교 정보공학과 졸업(박사)
2008년 7월~현재: 경기대학교 산업보안학과 산업기술보호특화센터 연구교수

김 재 성 (Jason Kim)
정회원
1986년 2월: 인하대학교 전산학 이학학사
1989년 2월: 인하대학교 전산학 이학석사
2005년 8월: 인하대학교 정보 통신공학과 공학박사
1996년 7월~현재: 한국인터넷진흥원(KISA) 지식정보보안산업팀 수석연구위원
2001년 2월~2007년 11월: TTA PG505 (바이오인식) 국내표준화 의장, JTC1 SC37 전문위원, KBA 사무국장
2006년 2월~2007년 11월: 아시아바이오인식컨소시움(ABC) 사무국장, ITU-T SG17 · JTC1 SC37에디터
2009년 2월~현재: ISO TC68/JTC1 SC37 전문위원, 한국정보보호학회 표준화이사, TTA국제표준전문가

김 귀 남 (Kuinam J. Kim)
정회원
1988년 2월: 캔자스대학교 수학과 졸업 (학사)
1992년 2월: 콜로라도주립대학 통계학과 졸업 (석사)
1993년 3월: 콜로라도주립대학 산업공학 졸업 (박사)
2000년 2월~현재: 경기대학교 산업보안학과 교수