특집 07

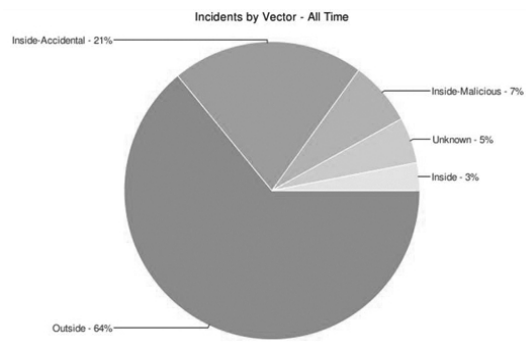
정보유출 탐지 기술의 동향 및 개인정보보호 관점에서의 고찰[1)]

목 차

김형종 · 김진형 · 이 알렉산더
(서울여자대학교)

1. 서론 및 동향

본래 정보보호의 핵심 이슈는 외부 공격자의 내부자원에 대한 침해와 이를 위한 취약점의 악용에 대한 대응에 있었다. 침입 탐지, 차단 및 방지시스템(IDS, Firewall, IPS) 등의 정보보호 제품군들의 주된 역할이 바로 권한 없는 사용자의 시스템자원에 대한 접근을 차단하는 것이다. 그러나, 최근 정보보호의 새로운 관심대상으로 내부자에 의한 정보 유출이 대두되고 있다. 특히, 국내 대기업들은 사내의 정보가 국외로 유출 될 때 발생하는 막대한 피해에 대해 심각히 대처하고자 하고 있으며, 이를 위한 다양한 보안 솔루션을 도입하였거나 도입을 계획 중이다. 최근에는 중요정보를 다루는 금융, 의료 분야 기관 및 핵심 지적 재산을 보호하기위한 대기업 뿐 아니라 정부 기관을 포함한 모든 기업 및 기관에서, 개인정보보호의 필요성으로 인해 개인식별정보(PII : Personally Identifiable Information)를 어떻게 관리 할 것인가에 대한 관리 대책을 고심하고 있다. IDC 보고서에 따르면, 기업의 보안사고가 공표됨으로 인해 생기는 피해의 규모는 기업이 하루 동안 업무를 수행하지 못하는 정도의 피해규모와 큰 차이가 없다고 조사된 바 있다[1].

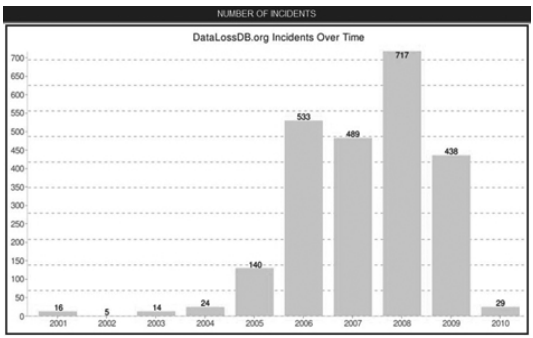


(그림 1) 내부정보 유출의 원인 요소들

내부자가 정보를 유출 시키는 이유는 의도적인 경우와 과실로 인한 경우로 나눠질 수 있으나, 정보의 유출을 방지하고자 하는 입장에서는 동일하게 다루어지는 것이 일반적이다. 정보 유출과 관련한 통계 정보 및 사고 정보를 다루는 OSF의 DATALABDB[2)]에 따르면, 2006년 이후

1) 이 논문은 2009년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(2009-0068361)

매년 400건 이상의 주목할 만한 정보유출 사고가 있었다는 것을 확인할 수 있다.



(그림 2) 정보유출사고 발생 건수

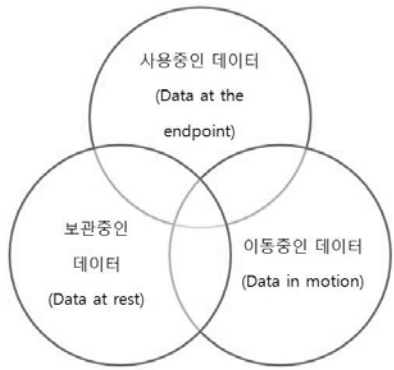
또한, 정보 유출의 주체 측면에서, 여전히 외부자로 인한 것이 64% 이지만, 내부자에 의해서 이루어졌다고 확신이 되는 상황이 전체의 31%로 파악이 되고 있다. 이러한 정보유출에 대한 상황을 고려할 때, 내부직원의 정보관리에 대한 체계 수립이 선행되어야 한다는 것을 알 수 있다.

정보유출 탐지 소프트웨어의 필요성과 관련하여서 IDC 보고서에 따르면, 정보유출에 대해 1,000명 이상의 직원을 둔 기업에서는 정보유출 방지 관련 솔루션을 도입해 둔 상태이기 때문에 이로 인한 두려움이 적었으나, 여전히 내부자의 악의적인 정보유출이 가장 큰 고민거리였다(52%). 500~1,000명 규모의 기업은 55%가 외부요인에 의한 데이터 손실을 가장 큰 고민으로 제시하였다. 데이터에 민감한 금융권의 경우 내부직원의 실수로 인한 손실을 가장 우려 했으며, 금융권 외의 수직시장[3]에서는 내부직원의 악의적인 정보유출을 가장 우려했다.

정보 유출의 원인과 관련하여, OSF의 자료에 의하면 60%이상이 무방비상태의 무선랜, 디폴트 패스워드, 시큐어코딩 기술의 미적용 등의 기술적인 취약점으로 기안하며, 40% 정도가 직원의 의도적인 혹은 무지에 의한 것으로 분석되고 있다. 이러한 원인들 중 본 고에서는 주로 내부직원의 특정한 의도에 의한 부분을 집중적으로 다루고자 한다.

2. 정보유출방지의 기본 개념

정보유출방지(DLP : Data Loss Prevention)란 회사로 하여금 중요 정보에 대한 정보흐름을 효과적으로 관리하기 위해 보안 정책을 수립, 운영 및 배포하는 것이다. 정보유출방지기술은 지적 재산권의 보호(Protection of Intellectual Properties)와 규정에 대한 준수(Compliance of Regulations)를 위해 필수적 기술로 여겨지고 있다. 정보유출방지기술에서 보호하고자 하는 데이터의 영역은 다음 3가지이다[2].



(그림 3) 정보유출 탐지대상 영역

- 사용 중인 데이터(Data at the endpoint) : 사용 중인 데이터는 현재 단말 시스템에 존재하는 정보로서, 계약서, 기업 간 합의서 (Term sheets) 및 기타 영업비밀정보 등이 될 수 있다. 이러한 정보들은 개인의 단말에서 다른 단말로 네트워크를 통하거나 혹은 오프라인으로 전송이 가능하다.

2) Open Security Foundation's Datalossdb(http://datalossdb.org)
3) 수직시장이란 유사한 제품이나 서비스들을 개발하는 산업이나 기업들을 말한다. 수직시장의 예로는 보험, 부동산, 금융, 제조업, 소매, 수송, 병원, 그리고 정부 등이 있다.

- 이동 중인 데이터(Data in Motion) : 이동 중인 데이터는 전자우편, 메신저, P2P (Peer to Peer), FTP (File Transfer Protocol) 및 웹 사이트 업로드 등의 데이터 전송방법을 통해 전달되고 있는 것을 말한다. 이러한 데이터를 보호하기 위해서는 데이터 이동의 모니터링, 암호화 및 차단 기술 등이 적용되어야 한다.
- 보관중인 데이터(Data at Rest) : 보관중인 데이터의 경우 앞에서 명시한 기업의 핵심 정보 중 현재 사용중이지 않은 정보를 말하며, 주로 파일서버, 개인 PC 및 노트북 컴퓨터, USB 드라이브 등에 저장되어 있는 상태의 정보들이다. 정보유출방지에서는 기업의 핵심정보가 어떤 단말 또는 저장장치에 저장되어 있는지 발견하고, 보호하는 역할을 수행해야 한다.

위와 같은 3가지 영역의 데이터를 보호하기 위한 기술은 단순히 정보보호기술 만으로 이루어질 수 없으며, 내부의 정보 흐름의 관리, 순응요구 규제들, 인적자원에 대한 교육 및 통제 등 매우 많은 영역의 문제가 고려되어야 한다. 특히, 정보유출방지기술의 기업 내 도입 및 적용을 위해서는 다음 3가지 정보보호서비스가 고려되어야한다.

- 정보보호 컨설팅 : 정보 유출을 방지하기위한 현 상태의 파악과 계획 수립을 위해 사전에 수행되는 위험 평가에 해당한다. 표준 정보보호 컨설팅 프레임워크에 따른 위험평가의 수행을 통해 체계적인 정보유출에 대한 대응기술 적용이 가능하다.
- 정보유출방지솔루션 구현 : 정보유출과 관련하여 컨설팅 과정에서 발견한 취약점을 해결하기 위한 기술적, 인적 및 업무 프로세스에 대한 정보유출 방지기술의 구현 단계이다.
- 보안 서비스 운영 : 구현된 정보유출방지솔루션을 효율적으로 운영하기 위한 절차이다. 사고의 발생을 원격에서 모니터링하게 할 것 인지 실시간 모니터링을 가능하게 할 것인지, 정보유출 상황 발생 시 대응을 어떻게 할 것인지 등에 대한 관리적 이슈가 논의된다.

이러한 정보 유출 기술이 사용될 수 있는 영역으로는 아래와 같은 4가지 상황들을 고려해 볼 수 있다.

- 정부 규제에 대한 순응이 필요한 경우 : 미국의 HIPPA, PIC-DSS와 같은 정보보호와 관련한 규제를 효과적으로 적용하기 위한 실용적 기술로 활용되는 경우이다.
- 지적 재산권의 보호가 필요한 경우 : 기업의 특정 아이디어에 대한 문서 및 설계도면과 같이 경쟁사에 유출시 큰 피해가 될 수 있는 경우이다.
- 영업 비밀에 대한 보호 : 기업 간의 계약서 및 합의서 또는 인수합병 관련 정보들이 이 경우에 해당한다.
- 허가된 것이지만 감시가 필요한 경우 : 기업 내의 특정사람 또는 조직에 대한 비방이나, 경쟁사로의 이직을 위한 이력서 제출 등의 경우이다.

3. 정보유출 방지 솔루션 동향

본 장에서는 정보유출탐지를 위해 요구되는 주요 기술을 설명하고자 한다. 정보유출탐지하기에 앞서 선행되어야 하는 중요정보의 정의 및 등록에 대한 설명은 아래와 같다.

- 중요데이터유형 정의 (Described Data) : 주민번호, 신용카드번호 등과 같이 중요 데이터의 유형을 정형화하는 것을 말한다. 이를 위해 정규식(Regular Expression) 및 검색식 등의 정보의 패턴을 표현하는 기법이 활용 될 수 있으며, 때에 따라서 다양한 지식 표현 기법이나 정보의 해쉬 값이 사용되기도 한다.
- 중요데이터를 등록 (Registered Data) : 중요정보의 데이터유형을 정의한 후 이에 해당하는 정보를 찾아 등록하는 작업을 말한다. 예를 들어 특정 기관에서 100만 건의 문서를 관리

보관 하고 있다면, 이중 "중요데이터유형 정의"에 만족하는 데이터로 어떤 문서들이 있는지를 찾아 등록하는 작업이 요구된다. 정보유출 방지 솔루션은 결국 등록된 중요데이터를 어떻게 관리할 것인지에 초점을 맞추게 된다.

이와 같은 정의 및 등록된 중요 정보에 대해 실제 정보유출방지 솔루션이 갖는 4가지 중요 구성요소를 통해 어떻게 중요정보가 관리되는지 설명하고자 한다.

3.1 중요정보 발견 모듈(Critical Information Discovery Module)

기관의 네트워크 및 시스템 내에 있는 중요정보는 관리자의 중요정보에 대한 정의에 따라 따로 분류 및 관리 되어야 한다. 이러한 중요정보의 분류 및 관리 기법은 매우 중요한 기술적 요소이다. 중요정보 발견모듈이 접근 가능한 모든 데이터에 대해 주기적으로 점검을 수행하여 중요정보를 선정하고, 중요정보에 대한 현재 위치, 중요정보 인덱스 및 해쉬 값 등을 관리해야한다. 현재, 대부분의 DLP 솔루션은 중요정보 발견모듈을 보유하고 있다. RSA의 "RSA DLP Datacenter", McAfee의 "McAfee Network DLP Discover", 시만텍의 "Symantec DLP Network Discover"와 "Symantec DLP Endpoint Discover"가 대표적인 것들이다 [3][4][5].

3.2 중요정보 모니터링 모듈(Critical Information Loss Monitoring Module)

이동 중인 데이터로는 e-mail을 통해 자료를 전송하거나 웹사이트에 데이터를 업로드 하는 경우를 포함한 네트워크를 통해 정보가 흘러가는 상태의 데이터들을 말할 수 있다. 이들은 다음 2가지로 분류 되며 각각에 대한 유출 방지 대책이 마련되어야 한다.

- 중요 데이터로 등록되어 있는 파일 또는 정보 단위 (information unit) : 중요데이터로 이미 등록되어 있는 정보를 외부로 전송하고자 할 경우, 이를 탐지하기 위한 메커니즘이 동작되어야 하며, 탐지된 경우 정보의 분류등급에 따라, 단순 로깅, 암호화를 하여 전송할지, 전송을 금지할지를 결정하게 된다.
- 사용자가 전송 시점에 작성한 정보 : 사용자가 직접 작성한 문장 및 단어들에 중요정보로 표현된 내용이 있는지를 탐지하여 유출 방지에 활용하는 경우이다.

이동 중인 데이터의 유출 방지 솔루션으로는 RSA의 "RSA DLP Network" 모듈이 이에 해당한다. RSA는 특히 CISCO의 네트워크 장비에 탑재된 솔루션을 출시하였다.[4] McAfee의 "McAfee Network DLP Monitor"는 네트워크에서 전달되는 패킷들을 분석하여, 로깅을 하는 기능을 주로 수행한다. 시만택은 "Symantec DLP Network Monitor" 모듈을 통해 다양한 네트워크 프로토콜에 대한 모니터링을 수행한다 [3][4][5].

중요정보의 모니터링에 있어서 개인 PC에서 사용 중인 정보(Data at an endpoint)에 대한 처리를 위한 별도의 도구들이 존재하며, 이들은 네트워크를 통한 정보의 외부 유출 뿐 아니라 USB 메모리와 같은 물리적 수단을 이용한 유출까지도 탐지하게 된다. RSA는 이러한 기능을 수행하는 시스템으로 "RSA DLP Endpoint"를 보유하고 있으며, McAfee는 "Host Data Loss Prevention"이라는 솔루션을 보유하고 있으며, 시만택의 경우 "Symantec DLP Endpoint Prevent"를 가지고 이러한 기능을 수행한다 [3][4][5].

국내 정보유출방지를 위한 제품들을 보면, 일반적으로 특정 응용프로그램을 대상으로 한 솔

4) CISCO C-Series에 임베드된 제품을 통해 e-mail을 통한 정보유출을 탐지, S-Series에 임베드된 제품을 통해 WWW에 올려지는 데이터에 대한 정보유출 탐지.

루션들이 주류를 이루고 있다. (주)소만사의 Mail-i, Msg-i, DB-i, Print-i, WebKeeper, ClickMind 등의 시스템들은 내부정보유출에 대한 응용 프로그램별 대응 기술을 가지고 있으며, Privacy-i의 경우 내부의 개인정보에 대한 유출에 대해서 대응한다. 닉스테크는 SafePC Enterprise라는 도구를 통해 PC의 통합관리 및 내부 정보 유출방지 기술을 제공하고, 특히 개인정보에 대한 유출방지를 위한 SafePrivacy라는 솔루션을 제공하고 있다. 그 밖에 SafeUSB를 통한 매체 등록 및 관리, SafeNotebook 도구를 통한 휴대용 컴퓨터의 분실로 인한 정보유출 방지 등의 기술을 제공한다. 두 개의 업체 모두 개인정보유출을 탐지하기 위한 솔루션을 가지고 있는 것은 최근 국내에서 발생한 대규모의 개인정보 침해사고에 기인한 것으로 볼 수 있다[6][7].

3.3 중요정보 유출 대응 모듈(Critical Information Loss Response Module)

정보유출에 대한 대응은 정보소유기관의 정책을 기반으로 동작된다. 일반적으로 중요정보에 대한 등급이 결정되면, 등급에 따른 대응 방법이 결정되게 된다. 예를 들어 고급비밀(Top Secret)에 해당하는 정보에 대해서는 외부로의 유출을 차단(Block) 하게 될 것이고, 비밀정보(Secret)에 대해서는 암호화(Encryption)를 수행할 수 있다. 관리대상정보(Classified)에 대해서는 외부로 송신된 정보에 대해 감사정보를 남기는(Auditing) 정도의 대응을 할 수 있다. RSA의 "RSA DLP Network" 모듈은 모니터링 기능 외에 대응 기능을 가지고 있으며, McAfee의 경우 "Network DLP Prevent" 모듈이, 시만택의 경우 "Symantec DLP Network Protect", "Symantec DLP Network Prevent", "Symantec DLP Endpoint Prevent"가 이러한 기능을 수행한다[3][4][5].

3.4 중요정보 유출 방지 관리 모듈(Critical Information Loss Prevention Manager)

중요정보의 유출 방지 솔루션들을 운영관리하는 모듈에 해당하며, 중요정보에 대한 정의 및 유출 정보에 대한 대응 이력 등의 정보를 조회할 수 있는 화면을 제공한다. 중요정보의 유출 이력 정보는 관리자 관점에서 매우 중요한 사용자 인터페이스로서, 유출 당사자에 대해 책임을 묻기 위한 중요 증빙으로 활용가능하다. 또한, 중요정보의 정의의 경우, 중요정보에 대한 유출 여부결정의 오류에 대한 결정적 역할을 하게 된다. 이는 오탐(False Positive Error) 또는 미탐(False Negative Error)의 오류의 발생이 중요정보의 정의가 어느 정도 잘되어 있는지에 의존적이기 때문이다. RSA의 "RSA DLP EM"과 McAfee의 "Network DLP Manager", 시만텍의 "Symantec DLP Enforce Platform"이 이러한 기능을 하는 모듈들이다[3][4][5].

4. 정보유출방지와 프라이버시 침해와의 관계

정보유출에 대한 탐지에 있어서 중요 이슈중 하나가 프라이버시 정보에 대한 외부 유출에 대한 관리에 있다. 이는 고객정보를 대량으로 보유하고 있는 주요 기관 혹은 회사들이 개인정보 유출에 대한 법적 책임을 다하는 관점에서의 필요성이다. 현재 정보유출과 프라이버시 침해 사이의 관계는 대부분 이러한 부분에 대한 해결책을 제시하는 것이었다.

반면, 다른 프라이버시 침해관점의 이슈로 고려할 수 있는 것은 내부자의 행위에 대한 모니터링이다. 내부자의 행위를 모니터링하는 것은 내부정보를 보호하는 관점에서는 매우 중요한 반면 내부자의 프라이버시를 보호하는 측면에서는 적절하지 않은 면이 있다. 내부자의 프라이버시 보호에 대해서는 내부자와 기업주와의 상호간의 인식 및 협약에 의해서 이루어져야 한다는 특성

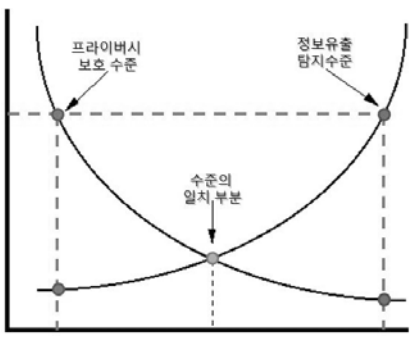
이 있다. 일정 규모이상의 기업의 경우, 노조가 이러한 협약의 대표자가 되는 것이 일반적이다. 이러한 협약에 있어서 중요한 점은 다음 2가지이다.

- 어느 정도까지의 내부자 정보 감시에 대해 허가를 할 것인가?
- 허가된 정보에 대해 어느 정도 내부자 개인의 신원의 식별이 어렵게 할 것인가?

위의 2가지 질문에 대한 기술적 대책으로 이후로 설명될 2가지 연구 주제를 생각할 수 있다.

4.1 내부자 정보감시에 대한 프라이버시 침해 정도 연구

내부자의 행위에 대한 모니터링은 사업주 관점에서는 정보보안을 위해 매우 당연한 조치라고 할 수 있으나, 내부직원은 이에 대해 매우 불쾌한 감정을 가질 수 있다. 이러한 문제를 최소화 하기위해 내부자에게 정보감시의 정도를 사전에 인지하도록 해주는 방법이 고려될 수 있다. 또한, 내부자에게 그러한 정보감시가 가져올 수 있는 회사 중요정보의 보호 효과를 정량화해서 보여줄 필요가 있다. 이를 위해서는 정보유출 탐지정도와 프라이버시 침해정도 사이의 상관관계를 보여 줄 수 있는 (그림 4)와 같은 모델이 필요하다. (그림 4)에서 볼 수 있듯이 두 가지 지표 사이의 관계는 서로 대립되는 요소로서 일정 수준의 균형점을 찾아야 하는 관계이다.



(그림 4) 프라이버시 보호 수준과 정보유출 탐지 수준의 개념적 상관관계

하지만 균형을 반드시 맞출 필요는 없다. 만일 특정 기업이 프라이버시 보호에 대한 모든 사항을 무시하면서, 정보유출에 대한 탐지를 수행하고자 한다면, 이러한 모델을 기반으로 기업의 내부직원에게 명확한 설명을 해 줄 수 있을 것이다.

4.2 감사정보에 대한 익명화 기술 적용

감사정보를 익명화 하는 기술은 중요정보의 유출대응 모듈에서 남긴 감사정보(Audit Record)에 대한 개인식별 방지 기술이라고 할 수 있다. 익명화를 위해서는 PII 정보에 대해 해쉬함수를 적용할 수 있으며, 익명화된 정보에 대해 추후 책임을 묻고자 하는 상황이 발생할 경우, 실사용자를 추적할 수 있는 기능을 부여할 수 있다.

5. 결 론

지금까지 정보유출방지기술의 필요성 및 현황을 살펴보고, 유출 방지를 위해 고려해야할 정보의 3가지 유형인 사용, 이동, 저장의 3가지 형태를 살펴보았다. 중요정보는 관리자에 의해 정보표현기법에 의해 표현이 되어야 하며, 이렇게 표현된 주요정보의 정의를 기반으로 현재 관리대상 시스템 및 네트워크에 존재하는 중요정보에 대한 등록이 필요하다. 등록된 중요정보에 대한 관리와 함께 내부자가 실시간으로 작성하는 문구 또는 메시지에 있을 수 있는 중요정보에 대해서도 모니터링이 되어야 한다. 이러한 중요정보의 유출을 막기 위한 솔루션들이 국외 업체를 중심으로 개발 시판되고 있으며, 국내 일부 업체 역시 활발히 관련 솔루션의 개발을 서두르고 있다. 정보유출 방지를 위한 기술을 적용할 경우 정보수집과정과 로그를 남기를 과정에서 내부자의 행위를 감시하는 상황이 발생하고 이로 인해 프라이버시 침해가 이루어질 수 있다. 기본적으로 내부자 정보 유출을 차단하기 위한 기술은 프

라이버시의 일부 침해를 감수해야하지만, 정보의 소유자에게 어느 정도의 개인정보에 대한 조회가 이루어질 수 있는지와 왜 그러한 상황이 발생하는 지를 설명할 수 있어야 하며, 이를 위한 모델이 필요하다. 또한 개인정보유출과 관련된 상황의 인지를 위한 감사기록에 대해 익명화 기술을 적용할 경우 기록의 일부가 유출되더라도 이로 인한 프라이버시침해의 정도는 덜해질 것이다.

참고문헌

[1] Eric Comage, Jozef Gemela, "Business Value of Data Loss Prevention", Executive Brief, IDC, September 2009

[2] Rich Mogull, "Understanding and Selecting a Data Loss Prevention Solution", SANS Institute, 2007

[3] http://www.rsa.com/dlp

[4] http://www.mcafee.com/us/enterprise/products/data_protection/data_loss_prevention/

[5] http://go.symantec.com/vontu/

[6] http://www.somansa.co.kr

[7] http://www.nicstech.co.kr

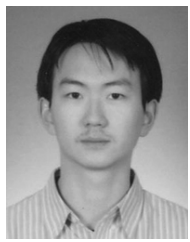
저자약력

김 형 중

1996년 성균관대학교 정보 공학과(공학사)
1998년 성균관대학교 정보 공학과(공학석사)
2001년 성균관대학교 전기전자 및 컴퓨터공학과(공학박사)
2001년~2007년 한국정보보호진흥원 수석연구원
2004년~2006년 Carnegie Mellon University, USA Visiting Researcher
2007년~현재 서울여자대학교 컴퓨터학부 조교수
관심분야 : 개인정보보호, 인터넷전화보안, 이산사건 시뮬레이션 방법론
이 메 일 : hkim@swu.ac.kr

김 진 형

2006년 2월 서울여자대학교 정보보호공학과 졸업
2008년 2월 서울여자대학교 대학원 컴퓨터학과(석사)
2008년 3월~현재 서울여자대학교 컴퓨터학과 박사과정
관심분야 : 정보보호, 개인정보보호, 디지털 포렌식
이 메 일 : jinny@swu.ac.kr



이 알렉산더

2002년 3월 Al-Farabi Kazakh National University, Kazah 입학
2007년 2월 Al-Farabi Kazakh National University, Kazah 졸업
2008년 3월~현재 서울여자대학교 컴퓨터학과 석사과정
관심분야 : 개인정보보호, 디지털포렌식
이 메 일 : eav-1@hanmail.net