情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

자동화된 침해사고 대응 시스템에서의 안전하고 합법적인 ISP의 IP 정보 제공 방안

김 현 상*, 최 운 호**, 이 석 희***, 이 상 진***, 임 종 인***

요 약

정보통신망 이용 촉진 및 정보보호 등에 관한 법률 개정에 따라 ISP는 해킹사고 관련 정보의 제공 및 신고가 의무화 되었다. ISP는 이를 이행하고는 있으나, 법률에서 정한바 대로, 관련 정보를 훼손·멸실 및 변경 등을 방지할 수 있는 조치를 취하고 있지는 않다. 따라서 본고에서는 ISP가 이러한 조건을 충족하면서도 자동화된 침해사고 대응 시스템과 고도화 되고 자동화 된 방법으로 정보를 공유를 하는 방안을 제시하였다.

Ⅰ. 서 론

최근의 정보보호 침해사고 특히 해킹 및 바이러스는 경제적 이익이나 정치적 시위를 위해, 민간 부분뿐만 아니라 국가 기관에 대해서도 조직적이고 체계적인 형태의 공격들이 급증하고 있다.

정보통신부는 이러한 경향에 대응하기 위해 2004년 7월 15일 국정원, 국방부, 경찰, 정보보호 업체 등이 참석한 가운데 '제1차 민간부문 해킹·바이러스 방지대책 협의회'를 열었다.[1] 이 자리에서는 국가 기관 및 민간 부분의 해킹사고 피해를 예방하기 위한 민관 합동 대응 전담 조직을 신설하고, 특히, 침해사고의 후속 조치와 발신지 추적을 위해, 주요 ISP 및 IDC의 해킹사고 관련 정보의 제공 및 신고가 의무화 되었다.

이에 따라 2004년 7월 30일 대통령령 제18505호와 정보통신부령 제155호에 의해 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 제10조의 3이 아래 표 1의 내용과 같이 신설되었다.[2] 이러한 법률을 따르기 위해 ISP 협회는 협회 홈페이지에 실무자들만 접속 할 수 있는 페이지를 만들어서 해외 불법 정보 관련 자료를 열람하고, 의견을 공유하고 있다.[3] 그러나 이러한 조치만으로 정보보호 침해사고 발생 동시에 관련 정보를 담당자 간에 즉각적으로 상호 통신하여 협조하는 방안을 수립하기 어려우며, 정보의 훼손, 멸실 및 변경을 방지하는 조치가 특별히 강구되어 있지 않다. 따라서 본고에서는 ISP가 정보보호 침해사고 관련 정보를 자동화된 침해사고 대응 시스템과 고도화 되고 자동화 된 방법으로 정보를 공유하면서도, 고객 프라이버시가 안전하게 보장되는 방안을 제시한다.

표 1. 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 제10조의 3

제10조의3(침해사고 관련정보의 제공방법) 법 제48조의2제2항의 규정에 의하여 침해사고 관련정보를 제공하는 자는 다음 각 호의 방법에 따라 침해사고 관련정보를 제공하여야 한다. 1. 정보통신부장관이 정보통신망의 특성, 침해사고 동향 등을 고려하여 정하는 제공방식에 적합할 것 2. 침해사고 관련정보의 훼손·멸실 및 변경 등을 방지할 수 있는 조치를 취할 것 3. 필요시 정보통신부장관이 정하는 암호기술을 적용할 것 4. 그 밖에 정보통신부장관이 정하여 고시하는 방법·절차에 적합할 것

본 연구는 대학 IT 연구센터 육성 지원 사업에 의해 수행 되었습니다.
* 고려대학교 정보보호 대학원(GSIS)/정보보호 기술 연구센터(CIST) (neoshine@cist.korea.ac.kr)
한국정보보호학회 조기경보시스템연구회 WG07 "로그기록을 중심으로한 네트웍/시스템 포렌식" 부운영자
** 금융결제원 금융 ISAC실 정보보호평가팀장 (tiger@kftc.or.kr)
*** 고려대학교 정보보호 대학원(GSIS)/정보보호 기술 연구센터(CIST) ({gosky, sangjin, jilim}@korea.ac.kr)

Ⅱ. 침해사고 대응 시스템과 ISP의 협조

1. Source IP를 이용한 정보보호 침해사고 대응의 문제점

자동화된 침해사고 대응 시스템에서는 IPS, IDS, Firewall, Anti-Virus, 각종 네트워크 장비로부터 수집한 로그 및 이벤트를 수집, 이를 분석 및 가공하여 DB에 저장하게 된다. 이와 같이 기록되는 event 및 로그에 동일한 Source IP가 지속적으로 기록될 경우, 정보보호 관리자는 IP를 Black List에 등록해 접근을 통제하거나, IP 사용자에 대한 형사상의 수사를 사법기관에 의뢰하게 된다. 따라서 침해사고 발생 시 공격자를 식별하여 침해사고를 예방하거나, 침해사고 발생 시 사법기관이 컴퓨터 범죄 수사(Computer Forensic)를 진행하게 되는 핵심적인 디지털 증거로 Source IP 주소가 사용된다.[4,5] 그러나 이러한 정보보호 장비의 로그에 기록된 Source IP 정보만으로 공격자를 식별하고 수사를 진행하는 것에는 다음과 같은 단점이 있다.

첫째, 공격자가 유동 IP를 사용할 경우 침해사고의 정확한 통계를 추출하기 어렵다. 회사, 기관, 단체, PC방 등을 제외한 대부분의 개인 가입자들은 ISP에서 운영하는 DHCP 서버로부터 IP를 할당받는다. 이 경우 가입자가 사용하는 IP는 C class 까지 고정되어있고 하위 D class가 변화하는 형태이다. 만약 공격자가 유동 IP를 사용한다면, 정보보호 장비에 기록되는 IP가 수시로 변화한다. 따라서 정보보호 장비는 해당 IP가 과거의 유사 IP와 동일한 공격자로 식별하기 위해서 과거의 로그로부터 공격 유형의 유사도, 공격 대상 port, C class 동일성 여부를 검사하는 과정이 필요하게 된다. 이러한 검사 과정은 과거의 로그 DB를 수시로 열람하여 분석해야 하기 때문에 정보보호 장비의 과부하를 유도한다.

둘째, 공격자가 무선 인터넷을 사용할 경우 물리적 위치추적이 어렵다. 무선 인터넷은 AP(Access Point)로부터 유동 IP를 할당받게 된다.[6] 그러나 무선 인터넷의 특성상 사용자는 항상 동일한 AP만을 사용하지 않으므로, C class 동일성을 검사하는 방법은 의미가 없다. 특히, 공격자가 위치를 이동하면서 공격을 실시하는 "이동형 사이버 범죄"[7]는 물리적 위치추적이 거의 불가능에 가깝다.

셋째, ISP가 시간대별 IP 할당 로그를 장기간 유지하는데 현실적인 어려움이 많다. 2004년 12월을 기준으로 우리나라 78개 ISP에 가입된 초고속 인터넷 서비스 가입자 수는 1200만이다.[8] 침입자의 개인 신상을 확인하기 위해서는 ISP가 시간대별 고객 IP 할당 로그를 유지하고 있어야 한다. 그러나 이 로그를 장기간 유지하는 것은 현실적인 어려움이 많다. 예를 들어 우리나라에서 가장 많은 가입자를 보유하고 있는 ISP의 경우 이러한 침해사고 정보를 제공하기 위해 610만여 명의 인터넷 접속기록을 DB화하여 보관하여야 하기 때문이다. 물론 이러한 로그들은 일정기간 보관이 되겠지만, 장기간 보관하는 것은 경제적 비용 문제 때문에 현실적인 어려움이 많다.

물론 단순한 Source IP 기록만으로 일정 수준의 정보보호 단계를 유지할 수는 있다. 하지만 금융, 의료/보건, 전력, 급수, 국방 기관과 같은 핵심 기반 시설 전산 시스템은 침해사고 발생 시 반드시 이를 탐지하고 공격자를 색출해야 하는 고수준의 정보보호 단계가 적용돼야 한다. 따라서 Source IP를 기록하는 방법이외에도 ISP와 적극적으로 협력하여, 공격자를 식별할 수 있는 추가 정보(Attacker Identification Additional Information - AIAI)를 기록/유지하여, 이를 분석하는 단계가 추가되는 것이 강력히 요구된다.

2. 자동화된 침해사고 대응 시스템과 ISP와의 연동을 통한 AIAI 서비스

2.1 AIAI 서비스의 절차

본고에서는 위에서 설명한 공격자 식별 추가 정보(AIAI)로써 ISP 가입자 신상 정보(ISP Subscriber Personal Information - ISPI)를 활용하는 것을 제시한다. 개략적인 절차는 다음과 같다.

- □ ISP는 평시에 고객의 개인정보(가입자 주소, 이름)와 ISP만이 알고 있는 비밀키로 해쉬한 값(MAC - 키를 사용한 해쉬[9])을 계산하여 고객 정보 DB에 기록한다.($\mathbf{AIAI} = MAC_{key}(\mathbf{ISPI})$)
- □ 자동화된 침해사고 대응 시스템은 Firewall, IDS, Anti-Virus와 같은 정보보호 장비와 Router, Switch와 같은 네트워크 장비로부터 발생한 Event, Log들로부터 침입 탐지 내용을 분석하여 하나의 ESM 로그를 발생한다.
- □ 만약 ESM에서 High Alert(또는 Red Alert)가 발생하였다면, Event의 Source IP를 관리하는 ISP의 AIAI Server에 IP 주소를 암호통신으로 전송한다.

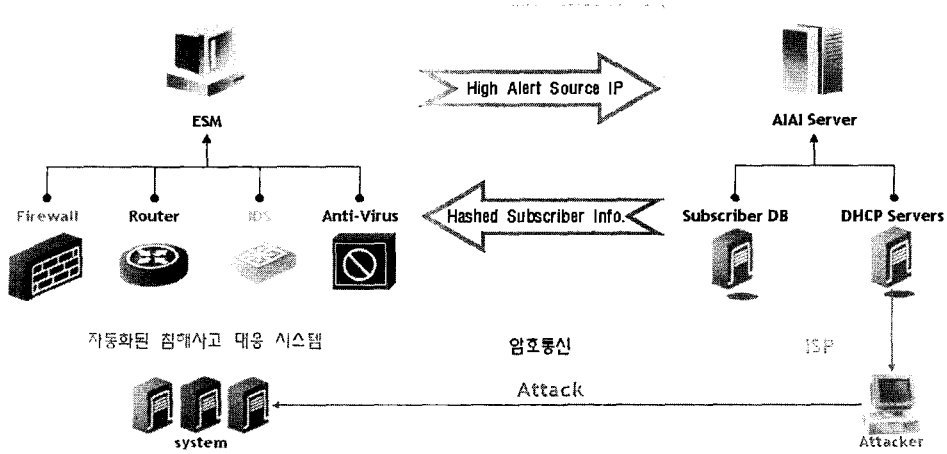


그림 1. 자동화된 침해사고 대응 시스템과 ISP와의 연동을 통한 AIAI 서비스의 구조

- ISP의 AIAI Serrver는 DHCP Server로부터 현재 IP를 사용하는 가입자를 확인하고, 고객정보 DB에서 AIAI값을 추출하여, ESM에게 암호통신으로 전송한다.
- ESM은 해당 Event Log에 AIAI 값을 기록한다. ESM의 Event 로그는 아래 표와 같은 형식을 가지게 된다.
- 추후 ESM 로그 분석결과 자동화된 정보보호 시스템에 침입을 시도한 공격자의 AIAI 값이 X_{128}라면, 적법 절차를 거쳐, ISP에게 해당 AIAI 값을 가지고 있는 사용자의 신원 정보를 요구한다.
- □ ISP는 사용자 고객 DB에서 해당 AIAI 값을 가지는 사용자를 검색하고, 해당 사용자의 세부 정보를 제공한다.

아래의 표 2에 기록된 ESM Log 예는 2005년 1월 23일 15시 23분경 23x.19x.10x.163 시스템에 Port Scan 공격을 실시하고 동일 18시 15분에 재차 공격을 시도한 것을 탐지하여 ISP로부터 획득한 AIAI 값을 기록한 뒤, 추후 사고 분석을 위해 로그를 AIAI 값을 기준으로 각 필드를 확장 정렬한 결과를 나타내고 있다. AIAI 값을 기준으로 정렬한 결과만으로도, 동일 공격자가 Port Scan을 실시했음을

표 2. AIAI 값을 추가한 ESM 로그의 예

No	Date	Source IP	Source Port	AIAI Value	Destination IP	Destination Port	Protocol	Detection
121	2005 01-23 15:23:05	16x.21x.16x.177	2965	C46D82849A105D11 59E654016ED517A0	23x.19x.10x.163	4899	TCP	port Scan (High)
122	2005-01-23 15:23:05	16x.21x.16x.177	2965	C46D82849A105D11 59E654016ED517A0	23x.19x.10x.163	4900	TCP	port Scan (High)
123	2005-01-23 15:23:06	16x.21x.16x.177	2965	C46D82849A105D11 59E654016ED517A0	23x.19x.10x.163	4901	TCP	port Scan (High)
124	2005-01-23 15:23:06	16x.21x.16x.177	2965	C46D82849A105D11 59E654016ED517A0	23x.19x.10x.163	4902	TCP	port Scan (High)
125	2005-01-23 15:23:07	16x.21x.16x.177	2965	C46D82849A105D11 59E654016ED517A0	23x.19x.10x.163	4903	TCP	port Scan (High)
627	2005-01-23 18:15:05	20x.11x.6x.169	2965	C46D82849A105D11 59E654016ED517A0	23x.19x.10x.163	4904	TCP	port Scan (High)
628	2005-01-23 18:15:05	20x.11x.6x.169	2965	C46D82849A105D11 59E654016ED517A0	23x.19x.10x.163	4905	TCP	port Scan (High)
629	2005-01-23 18:15:06	20x.11x.6x.169	2965	C46D82849A105D11 59E654016ED517A0	23x.19x.10x.163	4906	TCP	port Scan (High)

쉽게 판단 할 수 있으며, AIAI 값이 동일함에도 A class IP 주소가 서로 다르므로, 공격자는 무선인터넷을 사용하는 사용자임을 추측할 수 있다.

2.2 AIAI 서비스의 장점

이렇게 ISP 가입자 신상 정보를 공격자 식별 추가 정보로 사용하면 다음과 같은 장점을 제공한다.

첫째, AIAI 값을 공격자를 식별하기 위한 기준으로 삼을 수 있다. 사용자가 유동 IP를 사용하여, IP를 변화해가며 공격을 실시할지라도, ISP 가입자 신상 정보는 변하지 않는다. 따라서 특정 기간 동안 가장 많은 Event를 기록한 AIAI 값을 확인한다면, 비록 IP가 동일하지 않더라도, 같은 사용자임을 확인할 수 있다.

둘째, ISP가 고객 IP 할당 로그를 특정 기간이 지나 삭제하더라도, 당시 IP 사용자의 신원을 확인 할 수 있다. ESM에 기록된 AIAI 값은 ISP의 고객 DB에 지속적으로 유지되므로, 언제든지 침입자의 신원을 확인할 수 있다.

셋째, AIAI Server를 ISP의 정보보호 서비스 모델로 적용할 수 있다. 자동화된 침해사고 대응 시스템이 적용된 정보통신 국가 핵심 기반 시설의 전산망뿐만 아니라 민간 기업에게도 AIAI Server를 유료로 서비스 할 수 있다. 그렇다면, 민간 기업은 자신의 시스템에 침입한 공격자의 AIAI 값을 사법기관에 제공할 수 있으므로, 보다 확실한 정보보호 침해사고 후속 조치를 취할 수 있게 된다.

2.3 AIAI 서비스의 안전성과 합법성

이러한 ISP의 AIAI 서비스는 다음과 같은 이유로 안전성과 합법성을 보장하게 된다.

첫째, 올바른 AIAI 값은 오직 ISP만이 작성할 수 있으므로, 신뢰성을 보장한다. 만약, 특정 사용자 정보를 AIAI값으로 위조하기 위해서는 ISP 가입자 신상정보(ISPI)이외에도 ISP만이 알고 있는 개인키를 알아내야 한다. 그러나 키를 이용한 해쉬(MAC)는 블록 암호를 사용하고, 위의 절차에서 본 메시지 이외에 개인키가 노출되는 과정은 없으므로, AIAI 위조에 대한 어려움은 블록암호에 기지 평문 공격을 시도해 성공하는 만큼의 어려움을 가지게 된다.

둘째, 고객의 프라이버시가 보장된 상태에서 침해사고 대응 기관과 ISP와의 정보 교류가 가능해진다. 2004년 겨울 핸드폰을 사용한 수학능력시험 입시 부정사건 때, 각 통신사들로부터 수능 당일의 모든 메시지를 경찰이 입수하여 조사하였다. 당시 용의자 외의 일반 이동통신 사용자들은 자신의 민감한 정보가 동의 없이 기록되고, 또한 경찰이 열람하는 것에 대하여 적지 않게 항의했다. 이는 사이버 범죄 수사를 진행함에 있어서 용의자 이외의 무고한 사용자에 대한 프라이버시 문제는 민감하게 고려해야 할 사항임을 주지시켜주었다. 이러한 관점에서 볼 때, 고객 IP 할당 로그를 수사기관에게 통째로 넘겨주는 행위는 용의자 이외에 무고한 인터넷 사용자의 개인정보가 열람되는 행위로, 개인 프라이버시를 침해할 소지가 있다. 그러나 본고에서 제시하는 방식은, ISP가 고객 IP 할당 로그를 넘겨주지 않고 AIAI 값이 일치하는 용의자의 신상정보만을 수사 기관에 넘기므로, 수사 기관은 나머지 고객 정보를 열람할 필요가 없다.

셋째, AIAI 서비스는 법률의 테두리 내에서 합법적인 서비스임이 보장된다. 개인 정보보호 관점에서 또 한 가지 논의되어야 할 사항은 고객의 동의 없이 고객 개인정보를 가공하여, 제 3자에게 정보를 양도할 수 있는가에 대한 문제이다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 24조에는 "통계작성/학술연구 또는 시장조사를 위하여 필요한 경우로써, 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우 정보통신 서비스 이용 약관에 명시한 범위를 넘어 고객 정보를 이용하거나 3자에게 제공할 수 있다" 라고 명시되어있다.[2] 해쉬 함수의 특성상 해쉬값을 근거로 본래의 메시지(ISPI)를 추측할 수 없으므로, ESM에 기록된 AIAI 값만으로는 고객의 어떠한 정보도 추출해낼 수 없다. 따라서 AIAI 서비스는 정보보호 침해사고 통계 작성을 위해 고객의 정보를 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우에 해당하므로, AIAI 서비스 합법성이 보장된다.

2.4 AIAI 서비스의 한계

제시한 AIAI 서비스가 위와 같은 장점, 안전성, 합법성을 제공함에도 아래와 같은 몇 가지 제한을 가지고 있다.

첫째, 공격자가 네트워크를 우회하여 침입하여, ESM 로그에 Source IP가 Proxy Server, 내부 IP, 다른 피해 시스템의 주소로 기록되거나, 해외에 존재할 경우는 국내 ISP와 협조하여 AIAI 값을 획득하는 것이 불가능하다.

둘째, ISP의 AIAI 서버와 자동화된 침해사고 대응 시스템의 부하를 심각하게 고려해야 한다. 비록 High Alert의 경우에만 AIAI 서버에 질의(Query)를 전송한다 해도, 너무 많은 Event가 발생한다면,

AIAI 서버와 자동화된 침해사고 대응 시스템에 부하가 걸려 시스템 가용성에 문제가 생길 수 있다.

셋째, ISP에서 AIAI 서버 운영비용을 감수해야 한다. 물론 개정된 정보통신망 이용 촉진 및 정보보호 등에 관한 법률에서 의무화된 사항이긴 하지만, 각 국가기관과의 협조를 위해, 연결 서버를 증설하고, 그에 따르는 부하를 감수해야 한다는 측면은 소규모 ISP 업체들의 경우, 경제적인 어려움으로 작용할 수 있다.

이런 단점에 대한 대안적인 해결책은 다음과 같다.

첫째, 만약 공격자가 웹서비스를 사용한다면, 우회/은폐 IP에 대해서는 BPBT[10](Browser Plug-in Based Tracing) 역추적 기술을 적용하여, 실제 IP를 획득한다. BPBT 기술은 추적을 위해 클라이언트에 파일전송이나, 프로그램 설치를 필요로 하지 않고 브라우저의 플러그인에 구동명령을 전송하여, 소켓통신을 생성, 은폐한 IP 정보 값을 획득하므로, 적법성과 은밀성을 유지하면서도, 정확한 역추적 결과를 제공한다.

둘째, AIAI와 자동화된 침해사고 대응 시스템에 걸리는 부하는 적절한 시스템 증설과 정보보호 장비의 오탐(false positive)률 축소로 가용성을 확보할 수 있다. 특히 각 Event의 오탐률 축소는 AIAI 서비스 뿐만 아니라, 효율적인 정보보호 침해사고 대응을 위해서 꼭 필요한 부분이다.

셋째, ISP에 대한 경제적 비용 문제는 민간 부분에 대한 유료 AIAI 서비스에 의한 비용 회수와 국가 지원금을 통해 해결할 수 있다. 국가 정보통신 핵심 기반 시설들이 AIAI 서비스에 의해 정보보호 및 컴퓨터 범죄 수사에 결정적인 역할을 한다면, 이는 고수준의 정보보호 체계 유지에 따르는 소요비용 이므로 마땅히 국가가 일정부분 부담해야 할 것이다.

Ⅲ. 결 론

본고에서는 개정된 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 중 신설된 ISP 해킹사고 관련 정보의 제공 및 신고 의무사항과 그에 대한 ISP의 이행방안을 살펴보고, 이를 더욱 발전시켜, 자동화된 침해사고 대응 시스템과 고도화 되고 자동화 된 방법으로 정보를 공유하는 방안을 제시하였다.

제시된 방안은 자동화된 침해사고 대응 시스템이 침입을 탐지하였을 때, 공격자의 IP를 ISP에게 전송하면, ISP가 해당 IP 사용 고객의 신상 정보를 키를 사용한 MAC으로 해쉬한 AIAI 값을 전송하는 방식이었고, 이 값을 사용해 자동화된 침해사고 대응 시스템은 공격자를 식별하고, 추후 정보보호 침해사고 분석 및 컴퓨터 범죄 수사과정에서 ISP와 협조하여, 용의자의 신상을 알아낼 수 있는 장점을 제공하고 있다.

이러한 제시안이 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 제10조의 3-1에서 명시하는 정보통신부장관이 정해야 하는 정보보통신망의 특성, 침해사고 동향 등을 고려한 정보 제공방식을 결정하는데, 참고할 수 있는 자료가 되고, 사이버 테러 대응 센터와 같은 사법기관에서도 용의자 추적을 위한 새로운 기법으로도 참고가 될 수 있기를 바란다.

Ⅳ. WG07 소개

한국조기경보포럼의 WG07은 로그기록을 중심으로 한 네트워/시스템 포렌식 분과이다. 이 분과에서는 사이버 범죄는 급격히 증가하고 있는 반면, 이에 대한 사고 조사 기법은 피해의 속도와 규모를 따라가지 못하고 있다. 이러한 취지하에 사이버 범죄 조사 기법을 전문화시키고 예방하는 방안과 절차를 연구하며 컴퓨터 포렌식 실무자와 연구 인력의 협력 및 정보공유를 목적으로 하고 있다.

⊙ 연구 방향
- 각 조직별 분석 및 대응 기법의 공유
- 최신 사이버 공격 기법 분석
- 공격 분석 환경의 연구 및 구축

⊙ 분과 운영
- 월 1회 오프라인 모임을 갖고 연구 주제를 토론
- 연구희망내용 및 현장적용 내용을 자유롭게 발표

참 고 문 헌

[1] 전자신문, 2004년 7월 16일

[2] 정보통신부 홈페이지, http://www.mic.go.kr/network/inf/law/index.html

[3] 한국 ISP 협회 홈페이지, http://kispa.or.kr

[4] 최운호 "종합 침해사고 대응 시스템의 전체 구성", 금융 결제원

[5] 박광철, 최운호, 임종인, "종합 침해사고 대응 시스템에서의 블랙 리스트 추출방법과 관리방안 연구", KoreaCrypt 2005

[6] 무선 인터넷 개론, 이정환, 삼양출판사, 2001

〔7〕 디지털타임스, 임승택 사이버 테러 대응 센터장 인터뷰, 2004년 10월 20일
〔8〕 한국인터넷진흥원(NIDA), 2004년 12월 인터넷 통계 월보, http://www.nida.or.kr
〔9〕 Douglas R. Stinson, "Cryptography - Theory and Practice", pp.304~306, CRC Press
〔10〕 김태봉-2004 한국 조기경보 포럼, 최신 역추적 기술의 적용과 시연, 2004년 12월 14일

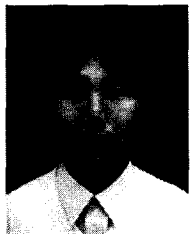
〈著 者 紹 介〉

김 현 상 (Hyun-Sang Kim)

2002년 : 경희대학교 학사
2004년 : 고려대학교 정보보호 대학원 석사
2004년~현재 : 한국정보보호학회 조기경보시스템연구회 WG07 "로그기록을 중심으로 한 네트워/시스템 포렌식" 부운영자
2005년~현재 : 고려대학교 정보보호 대학원 박사과정
〈관심분야〉 컴퓨터 포렌식, 조기경보, 침해사고 후속조치 자동화, 분산처리 컴퓨팅

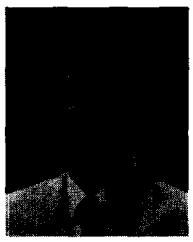
최 운 호 (Un-Ho Choi)

1990년 : 광운대학교 학사
1995년 : 광운대학교 대학원 전자계산학과 석사
2004년 : 한세대학교 대학원 정보보호공학과 박사
1989년~1996년 : 한국전산원 선임연구원
1996년~2001년 : 한국정보보호진흥원 팀장
2002년~현재 : 금융결제원 금융ISAC실 정보보호평가팀장
2003년~현재 : 한국정보보호학회 이사
2004년~현재 : 한국정보보호학회 조기경보시스템연구회 위원장
2004년~현재 : 국가정보보안협의회 조기경보시스템연구회 위원장
〈관심분야〉 조기경보, 블랙리스트, 관제센터운영, 침해사고신고 자동화 등



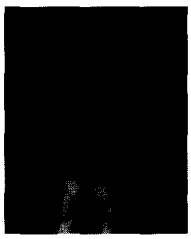
이 석 희 (Seok-Hee Lee)

2003년 : 부경대학교 컴퓨터공학과 학사
2004년~현재 : 고려대학교 정보보호 대학원 석사과정
〈관심분야〉 컴퓨터 포렌식, xml 보안



이 상 진 (Samgjin Lee)

1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구원 선임연구원
1999년 2월~2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 9월~현재 : 고려대학교 정보보호대학원 부교수
〈관심분야〉 대칭키 암호의 분석 및 설계, 정보은닉이론, 컴퓨터 포렌식



임 종 인 (Jong-in Lim)

1980년 2월 : 고려대학교 수학과 학사
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1986년 3월~2001년 1월 : 고려대학교 자연과학대학 정교수
2001년 2월~현재 : 고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터 센터장
〈관심분야〉 정보보호 이론, 정보보호 정책