通信情報保護學會誌
第6卷 第3號, 1996. 9

정보범죄의 추세와 대처 방안

최 영 호*

제 1 장 서 론

1. 정보범죄의 의의

오늘날 전 세계의 모든 컴퓨터는 정보에 대한 단순한 호기심 차원이 아니라 수많은 적대적 동기를 포함한 유능한 해커들과, 종래의 전통적인 범죄행위들을 컴퓨터를 통하여 실현하려는 잠재적인 범죄자들로부터 광범위한 공격의 대상이 되어가고 있으므로 어떤 학자는 이러한 사회현상을 "정보전쟁(Information Warfare)"이라고 까지 표현하고 있다.[1]

정보화 사회가 시작되면서 우리사회에는 정보범죄 또는 컴퓨터범죄라는 신조어가 사용되고 있지만, 학문적으로나 법률적으로 이에 대한 정확한 개념이 확립된 바는 없다.

원래 정보란 사물의 형편이나 사건의 진행상황을 의미하지만, 정보화촉진기본법 제2조 제1호가 "정보라 함은 특정한 목적을 위하여 광 또는 전자적 방식으로 처리하여 부호, 문자, 음성, 음향 및 영상등으로 표현한 모든 종류의 자료 또는 지식"이라고 정의하고 있는것처럼 정보화 사회에서는 단순한 자료(Data)와 정보(Information), 지식(Knowledge) 사이의 개념이 불명확하게 되었다.

따라서, 필자는 이러한 경향을 중시하여 정보범죄를 컴퓨터의 정보처리기능이나 컴퓨터가 처리, 보관, 전송하는 정보를 이용하거나 이러한 기능.정보에 대한 범죄를 가리키는 좁은 의미의 컴퓨터범죄를 포함하는 새로운 유형의 범죄행태로서 위와 같은 정보를 이용한 범죄와 정보에 대한 범죄를 총칭하는 넓은 의미로 정의하고저 한다.[2]

2. 정보범죄의 범주

정보범죄를 이러한 의미로 정의한다면, 정보범죄는 침해당하는 법익의 종류에 따라 다시 재산권 침해행위, 인격권 침해행위, 국가적 법익 침해행위의 세 종류로 나누어 볼 수 있을 것이다.

재산권 침해행위란 컴퓨터 사기, 컴퓨터를

* 법무부 법무연수원 검사

1) Winn Schwartau, Information Warfare, Chaos on the Electronic Superhighway, Thunder's Mouth Press, 1994, pp.3-4.

2) 산업 스파이행위와 프라이버시 침해행위의 대부분이 컴퓨터와 관련하여 이루어지는 것이 보통이지만, 반드시 컴퓨터를 전제로 하는 것은 아니므로 그 전부가 컴퓨터관련 범죄현상이라고 단언하기는 어렵다. 자세한 것은 졸저, 컴퓨터와 범죄현상, 컴퓨터출판사, 1995, pp.23-25, 참조

이용한 업무방해, 컴퓨터 스파이(Computer Spy), 컴퓨터 사보타지(Computer Sabotage) 등과 같이 컴퓨터를 이용한 경제적 이득의 불법적 취득행위나 컴퓨터에 대한 물리적 공격을 지칭하고, 인격권 침해행위란 컴퓨터에 의하여 처리, 보관, 전송되는 개인의 사생활 즉, 프라이버시(Privacy)에 대한 불법적 침해를 의미하며, 국가적 법익 침해행위란 국가의 안전보장에 관한 컴퓨터정보나 국제적 정보에 대한 불법수집, 탐지행위 또는 소위 "전자민주주의(Electronic Democracy)"에 불법으로 간섭하여 여론을 조작하는 행위 등을 지칭하기로 한다.

3. 정보범죄의 중요성

정보범죄는 다른 사람의 생명이나 신체에 아무런 위해를 가하지 않는 상태에서도 거액의 경제적 이익을 취득할 수 있고, 정보범죄의 대부분은 컴퓨터를 이용하여 이루어지므로 범행에 대한 발각이나 입증이 곤란하며, 컴퓨터의 자동적 결과처리, 또는 공간적 제한이 없는 광범위한 결과야기 가능성등을 이용하여 반복범행 또는 계속범행이 용이하다.[3]

따라서, 정보범죄는 위와 같은 특성으로 말미암아 엄청난 경제적, 사회적 영향을 초래하기 마련이다.

미국의 보험 서비스협회는 미국에서 컴퓨터 사기행위로 인한 연간 피해액만도 '95년에 80억 달러에 달하였고, 2,000년에는 200억 달러에 이를 것으로 전망하였지만, 정보범죄는 이와 같은 대규모의 경제적 손해 이외에 가공할만한 사회적, 문화적, 국가적 역기능을 초래할 수 있다.

국가의 안보, 외교 등에 대한 주요정보나 산업정보의 유출, 통신망에 대한 불법도전으로 인한 사회의 혼란과 정보질서의 문란등 사회적 역기능, 컴퓨터를 통한 도박, 음란물의 전파와 유통에 따른 문화적 역기능, 완전범죄 가능성에 대한 오신과 한탕주의 또는 새로운 범죄도구에 대한 호기심을 기초로 한 범죄로의 유혹, 그리고 다른 사람의 사생활에 대한 침범 등에 따른 윤리적 역기능 등이 그것이다.

제 2 장 정보범죄의 실태

정보범죄는 컴퓨터의 입,출력 조작에 의한 사기행위(Fraud by Computer Manipulation)를 비롯하여 소프트웨어의 불법복제(Software Piracy), 컴퓨터 스파이(Computer Spy), 프라이버시 침해(Infringement of Privacy) 등 전형적인 컴퓨터범죄 이외에도 종래의 전통적인 범죄에 컴퓨터를 행위의 수단으로 이용하는 범죄수법들이 대거 등장하고 있다.

특히, 자연재해나 복잡한 기계에 대한 통제체제가 전산화됨에 따라 국가적, 사회적 법익에 대한 침해 가능성이 점차 높아져가고 있음은 크게 주목할만한 사회현상이다.

1. 컴퓨터 조작사기

전세계적으로 확산일로에 있는 POS(Point-of-sale: 판매시점 재고관리 시스템), EFTS(Electronic Funds Transfer Systems: 전자자금 결제제도) 등 상업, 금융자료에 대한 자료조작(Data Diddling) 또는 컴퓨터 프로그램(Computer Program) 자체에 대한 트로이안 호스(Trojan Horse), 운영자로의 위장(Superzapping), 쪽문 만들기(Trap Doors), 논리폭탄(Logic Bomb), 시범 또는 표본으로의 위장(Simulation & Modeling)등 수법[4]에 의한 프로그램 조작은 정보범죄의 특성에 따라 쉽게 발각되지 않고, 장기적으로 반복범행되고 있다.

3) 상세한 것은 졸저, 전게서, p.26 이하 참조.
4) 상세한 범행수법에 대하여는 졸저, 전게서, p.31.이하 참조.

한편, 신용거래가 확산되면서 대량유통되는 신용카드의 자기 스트립에 기재되는 신원확인 번호(PIN: Personal Identification Number)를 조작하는 신용카드 위조행위가 증가함에 따라 신용카드 회사들은 자기 스트립에 카드회사의 컴퓨터로만 입력자료를 읽을 수 있도록 신용카드에 CVI(Card Value Identification)나 CVC(Card Value Code) 등의 보안장치를 하거나 홀로그램(Hologram)[5] 장치까지 동원하였지만, 이러한 보안장치마저 완벽하지 못함이 드러나 신용카드를 비롯한 모든 증거증권들이 IC Chip을 내장한 스마트카드(Smart-Card)로 전환될 전망이다.[6]

국내에서도 1995년 말에 외국인까지 개입한 국제적인 신용카드위조단이 적발되었고, 1988년부터 1994년까지 자그마치 6년동안 예금계좌를 허위로 조작하여 46억여원을 횡령한 시골 우체국의 한 여직원이 구속되기도 하였다.

2. 소프트웨어 불법복제

컴퓨터 프로그램은 제작자에게는 높은 부가가치를 창출하여 주고, 다양한 기능과 놀라운 성능으로 일반인들의 사용욕구를 가속시킴으로써 그 수요가 급격히 신장하고 있다. 세계 소프트웨어 시장은 1994년에 시스템 소프트웨어(System Software) 약 220억불을 비롯하여 모두 약 780억불에 달하였고,[7] 1995년에는 1,000억불을 초과하였다.

컴퓨터 프로그램 저작권에 대한 각국간의 마찰이 계속되고, UR협상에 따른 WTO(World Trade Organization: 세계무역기구)의 출범으로 '95. 7.1.부터 발효된 교역관련 지적소유권에 관한 협정[8] 등 국제간의 협약들이 불법복제를 금지하고 있음에도 프로그램의 복제 용이성과 복제행위에 대한 적발 곤난성 때문에 프로그램 무단복제행위는 근절되지 않고 있다.

세계 소프트웨어 연합회(Busines Software Alliance)에 따르면 '94년 미국기업들은 소프트웨어 불법복제로 150억달러 이상의 소프트웨어들을 약탈당하였다고 하는데[9], 비록 불법이라 하더라도, 많은 사람들은 엄청난 금액의 프로그램 대금을 지급하기 전에 주변사람으로부터 프로그램을 무료 또는 낮은 가격으로 복제하려는 것이 보통이므로 이러한 수요를 상업적으로 이용하려는 상혼들의 복제영업은 자연히 고도의 복제기술까지 동반하기에 이르렀다.

그러나, 이에 대한 프로그램 제조업자들의 방어도 만만치 않아 미국에서는 1995. 3. 역 어셈블링(Disassembling)[10]이 불가능하거나 복사횟수를 제한하는 복제방지 프로그램(Copy-Protected Software)까지 등장하였지만, 이러한 복제방지장치에 대한 격파작업(Unprotecting Technology)도 동시에 진행되고 있다.

우리나라에서도 컴퓨터 통신을 통한 온라인(On-line) 판매는 물론, 기록용(Writable) CD ROM[11]을 이용한 조직적인 불법복제가 횡행하고 있다. 특히, 인터넷(Internet)의 상용화로 그 사용자가 급격히 신장하고, 신용카드제도와 전자거래(Electronic Commerce)의 결합에 편승하

5) 간섭성이 좋은 레이저광선을 이용하여 물체로부터 반사하는 반사광, 투과광과 레이저로부터의 직접광(참조광)을 간섭시켜 감광자료에 간섭무늬가 기록되게 하는 것으로 여기에 또다른 빛(재생광)을 접촉시키면 원래 물체가 존재할 때와 동일한 파면이 재생되어 입체상을 볼 수 있게 된다.

6) 상세한 것은 졸저, 전게서, p.33. 이하 참조.

7) 'IDC보고서', 하이테크정보 제141호, 주식회사 하이테크정보, 1995.4. pp. 96-97.

8) TRIPS : Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods.

9) 중앙일보, '96. 5.23.자 10면 참조.

10) 이진화일로 컴파일(Compile)된 원시코드(Object Code)를 분석하여 소스코드(Source Code)를 알아내는 방법.

11) Compact Disc Read-Only Memory

여 전자시장의 표본인 인터넷은 거대한 복사기가 될 가능성마저 배제할 수 없게 되었다.

3. 컴퓨터 스파이

한편, 자료의 유출(Data Leakage)이나 쓰레기 줍기(Scavenging), 비동기 침범(Asynchronous Attack) 또는 도청(Eavesdropping, Wiretapping) 등에 의하여 이루어지는 컴퓨터 스파이는 기업이나 국가의 장래에 치명적인 손해를 가하고 있다.[12] 미국은 일본, 한국등의 컴퓨터 스파이 행위로 말미암아 연간 1,000억불 이상, 독일은 연간 80억 마르크 이상의 손해를 입고 있는 것으로 보고되었다.

특히, 이동통신기기와 멀티미디어 기술의 대중화에 따라 반도체기술이 정보산업에서의 중요성이 부각되고, 세계 반도체시장의 규모가 1994년에 1,464억 달러, 1995년에는 2,103억 달러에 달할만큼 무역시장에서 차지하는 비중이 커지자 그 제작기술에 대한 스파이행위가 국제적인 문제로 부상하였다.

급진하는 신기술을 바탕으로 한 과학장비에 힘입어 컴퓨터 스파이행위는 더욱 은밀하고, 정교한 방법으로 행하여지고 있다. 최근에 Intel의 기술진은 미국 정부가 암호화 알고리즘(Algorithm) 자체를 비밀로 분류할 정도로 완벽한 보안성을 자신하였던 클리퍼 칩(Clipper Chip)을 역공정(Reverse Engineering)[13]으로 제작할 수 있는 첨단기술을 개발하였고, 스마트카드 등 IC카드의 운영체제인 COS(Chip Operating System)에 대한 산업 스파이행위가 본격화한 것도 이러한 사실을 잘 대변해주고 있다.

미국 국방성은 '90년부터 라디오 방송보다 3,000배나 강한 17억W의 출력으로 가열한 극초장파(ELF)를 볼록렌즈화한 전리층의 하부로 통과시킨 다음, 전리층 상부에서 전파를 모아 반사함으로써 수 킬로미터의 지하까지 관찰이 가능하고, 레이더(Radar; RAdio Detecting And Ranging)가 포착하지 못하는 부분까지 탐지할 수 있게 되었다고 한다.

이러한 과학장비를 운용하고, 국가적인 이익을 쟁취하기 위하여 국가정보기관이 공개리에 전면에 나서기까지 이르렀는데 실제로 '95. 9. 미국의 CIA와 프랑스의 정보전자전부대(BRGE)는 정보수집, 판독능력을 갖춘 스파이를 공채까지 하였다고 한다.

4. 프라이버시 침해

가. 문제의 소재

조직이나 기업이 조직원과 고객에 대한 효율적인 관리와 비용절감을 위하여 작성하는 개인의 신상에 관한 자료들은 인권보호와 관련하여 중대한 의미를 갖는다.

은행의 전산자료에는 입,출금 내역, 부도내역, 자금사정, 신용상태 등이, 신용카드회사와 백화점의 전산망에는 개인에 대한 기본정보 이외에 카드사용에 따른 여행, 외식, 쇼핑 등 사생활에 관한 자료가, 병원의 전산기록에는 병력, 입원내력, 약물투입, 신경정신과에 관한 기록 등이, 행정당국, 세무당국, 수사,정보기관의 컴퓨터에는 직업, 직장, 직위, 재산사항, 최종학력, 출신학교와 학과, 전화번호, 의료보험 관련자료, 각종 면허보유내역, 병역사항, 가족사항은 물론, 소년기부터의 범죄경력, 주변인물, 친교관계, 반국가적 활동 등이 기록된다.

12) 상세한 것은 졸저, 전게서, p.43. 이하 참조.

13) 공개거래되는 반도체칩이나 컴퓨터 프로그램을 구입하여 칩의 도안이나 구조를 검색하거나 컴퓨터 프로그램의 Objetct Code를 PC의 Soucer와 같은 프로그램으로 Source Code를 알아내어 제조공정을 거꾸로 추적하므로써 칩의 디자인 설계나 프로그램의 실제 내용을 쉬게 알아내는 행위를 말한다.

이러한 자료들이 다른 사람에게 공개되면 심각한 인격권 침해를 야기하게 될 뿐만 아니라 자료의 분류와 정리과정이 잘못 처리된 경우에는 전산처리에 대한 완전무결성을 전제한 시세의 풍조로 인하여 해당정보의 관련자는 엄청난 피해를 입게되고, 이로 말미암아 소속 집단이나 사회, 국가에 대한 적대관계를 유발하기도 한다.

최근에 신용카드의 사용이 일반화되면서 신용카드를 이용한 항공기, 열차, 고속버스표 매표기록이나 음식점 거래내역을 통하여 개인의 사생활에 대한 정보가 다른 사람에게 누출될 가능성이 크게 높아졌는데[14] 가령, 신용카드를 이용하여 서점에서 서적을 구입한 경우, 그 거래내역은 POS에 의하여 자동기록되므로 동 기록을 검색한다면 소위 불온서적을 구입한 사람이나 반정부세력들의 인적사항이 전부 노출될 것이다. 또, 법원의 전산화가 완성되어 가옥명도 청구소송이나 대여금 청구소송을 당하였던 사람들 또는 의료과실로 인한 손해배상 청구소송을 제기하였던 사람들을 특정할 수 있다면 그들에게 돈이나 집을 빌려주지 않는다던지 진료를 거부하는 사태가 발생하지 않는다고 누구도 장담할 수 없을 것이다.

나. 사례

실제로 '92년 부산에서 노동쟁의 전력자에 대한 명부화일이 기업체들 사이에 전파되어 쟁의전력이 있는 사람들에 대한 취업이 거부된 적이 있고, '93년에는 심부름센터로부터 뇌물을 받고, 경찰의 주민조회나 범죄경력조회서를 함부로 출력하여 교부한 경찰관등 25명이 서울지검에 구속되었다.

또, '94년에는 구청이나 세무관서의 직원들이 자동차등록 관련자료와 세무관련자료를 유출하고, 백화점 직원들이 고액거래고객의 데이터베이스를 팔아넘겨 불특정 다수인으로 하여금 소위 "지존파"라는 살인마 조직이나 승객에 대한 강도강간을 일삼은 택시 운전사의 범행대상이 되게 함으로써 나라가 시끄러웠던 일도 있었다.

이러한 커다란 사고들이 있었지만, 아직까지도 은행이나 기업들의 거래내역을 인쇄한 컴퓨터 출력물이 지하철 주변의 노점상에서 포장용 봉투로 사용되고 있는 것을 보면 우리 전산관련 종사자들의 보안의식에 문제가 있음을 쉽게 알 수 있다.

1995. 1. 핀란드에서는 변태성욕자로 보이는 사람이 인터넷의 뉴스그룹(News Group)인 alt.religion.scientology 등에 동물이 소녀를 간음하거나, 아이들이 보는 앞에서 동물을 타살하는 내용들을 게재하여 핀란드 경찰이 위 뉴스그룹을 제작하는 컴퓨터 동호회를 수사하는 과정에서 한 동호회 개설자가 익명으로 송고하는 사람들의 인적사항을 경찰에 알려주었는데, 미국의 수사기관이 핀란드에 동 동호회 개설자에 대한 인적사항을 통보할 것을 요청하였으나 핀란드측이 사생활침해를 이유로 이를 거절함으로써 한동안 양국간의 외교문제가 되었던 일도 있다.[15]

미국은 연방통신법의 개정으로 1995. 4.부터 수화자가 발신인 자동확인(Caller ID 또는 CND, Calling Number Delivery)을 요구할 경우에 전화국은 발신인의 전화번호와 성명을 수화자에게 고지하여야 하는데 대부분의 자유업 종사자들이 집전화를 업무에 이용하고 있으므로 고객 등 거래처들이 자유업 종사자들의 집전화를 통하여 사생활을 침해하는 일이 많을 것이라고 우려하고 있다.[16]

14) 상세한 것은 졸저, 전게서, p.56 이하 참조.
15) Internet, Risks-l Forum, RISKS-1. 16.96, 1995. 4.
16) Erik Bloodaxe(Chris Goggans) 등, Phrack Magazine, Vol. 4, Iss. 47., 1995. 4.

다. 전망

산업사회의 구조가 점차 복잡다단한 법률관계로 얽혀지면서 조직과 개인간의 원활한 의사소통과 효율적인 업무처리 그리고, 기업의 고객에 대한 조직적인 관리와 광고효과, 능률적인 채권회수 등을 위하여 대부분의 신상자료가 전산정보화됨에 따라 이러한 자료의 불법적인 이용과 누설, 자료의 불법적인 수집과 저장, 부정확한 자료의 입력과 이용 등에 의한 프라이버시의 침해는 더욱 경계해야 할 대상이 되었다.

우리 신용정보의 이용 및 보호에 관한 법률은 신용정보의 불법수집, 조사행위(동법 제32조 제4호, 제15조)와 무허가 신용정보업을 금지하고(동법 제32조 제1호, 제6조), 공공기관의 개인정보보호에 관한 법률은 공공기관이 수집, 보유하는 개인의 정보화일을 함부로 누설하거나, 부당한 목적으로 사용하는 것을 금지하고 있지만(동법 제23조), 15대 국회의원 선거과정에서나 심지어는 과외학원까지 주민들의 인적사항, 가족사항, 컴퓨터 통신망 가입자의 인적사항등을 파악하여 서신이나 전자우편을 보낼 정도인 것을 보면 프라이버시 침해에 관한 우리의 현실은 매우 우려되는 상태라고 아니할 수 없다.

최신의 전자감시기술은 개방교도소 운영등에도 이용되지만, 인공위성을 이용한 프랙탈이론(Fractal Theory)[17], 영상확대장치(Image Amplifier)등 첨단기술까지 결합하여 개인의 사생활까지 감시할 수 있게 됨으로써 인권침해의 소지가 매우 높아지고 있다.

특히, 소프트웨어 제작회사들의 동종업자들에 대한 지나친 경쟁의식은 불법복제에 대한 증거자료를 확보한다는 명목으로 암암리에 사용자의 인격권을 침해하고 있는데 Windows '95의 옛날 버전이나 Netscape의 버전 2.0 이하의 것들에서 보는 것처럼 사용자에게 소프트웨어의 등록을 요구하면서 사용자에 대한 신상정보와 정품사용여부 등을 회사로 전송하도록 하는 비밀전송장치(일종의 Trapdoor)등을 내장하여 고객들에 대한 정보수집까지 이른 것은 새로운 양상의 인권침해로서 주목할 만하다.

5. 국가적·사회적 위기조장

항공기나 대형선박의 항법장치, 홍수통제, 우주비행관제, 핵관련시설의 통제등 교통,항행통제시스템 나아가 전기,전화등 국가기간동력과 통신운영체제 또는 무기체제의 운영에 대한 정보범죄는 국가적, 사회적 위기를 조장함은 물론, 특별한 경우에는 전쟁발발의 요인이 될 가능성마저 부인할 수 없다.

뒤에 설명할 "뻐꾸기의 알" 사건 외에도 1994. 11.과 12.에 발생한 영국인의 한국원자력연구소 전산망에 대한 침입행위, 네델란드의 암치료 센터의 핵관련 전산실에의 해커침입,[18] 한국전산원의 통신망에 대한 침입 등이 좋은 예이다. 또, 1983년 봄 콜로라도(Coloraro)강의 범람은 홍수통제 시스템의 가상설계(Modeling)가 잘못되어 발생한 것으로 확인되었고, 1987년 156명의 탑승객이 전원사망한 Northwest 255편의 충돌사고도 항법장치(Flight Simulator)의 오류에 의한 것으로 보도되었지만, 범죄행위에 의한 것인지는 밝혀지지 않았다.

한편, 전산관련자료의 조작은 아주 위험한 여론조작의 도구가 될 수도 있는데 1986년 필리핀의 대통령선거에서 행하여진 통계조작은 정권의 몰락까지 초래함으로써 전자 민주주의

17) 모든 형체는 일견 불규칙한 선의 연속으로 보이지만, 실제로는 규칙적인 변화의 연속이라는 이론.
18) 동 사건은 한국인이 범행한 것으로 보도되었으나 확인결과, 미국의 해커가 한국의 인터넷 사이트를 경유하여 범행한 것으로 밝혀졌다.

에 대한 좋은 교훈이 되었다.

현대국가에 있어서 정보범죄에 행하여지는 수단들은 군사,외교정보에 대한 도청과 스파이 행위, 무기체계에 대한 방해책동이나 무력화 등 군사작전의 도구로 이용되고 있다.[19]

미국 국방성은 종래의 전투행위와는 전혀 다른 의미의 군사작전, 소위 "OOTW(Operations Other Than War)"라는 이름으로 정보전쟁을 위한 군사적 연구를 진행하고 있고, 버지니아 워렌튼에 있는 미 육군의 Signal Warfare센터는 실제 전투에 사용할 컴퓨터 바이러스의 개발을 위해 전문가까지 초빙한 것으로 보도된 바 있다.

또한, 중동전쟁 당시 어느 국가의 행위인지는 밝혀지지 않았으나 Iran의 Air Bus 항공기에 대한 항법장치를 통제하는 컴퓨터 프로그램(FMS: Flight Management System)이 조작, 변경되어 동 항공기의 이,착륙이 방해되었던 일도 있다.

6. 종래 전통범죄에의 악용

가. 음란물 판매, 전시

불법복제 기술의 발달, 다양한 저장매체의 보급과 함께 인터넷이 대중화되면서 복제된 음란정보가 대량전파되고, 음란정보를 저장한 인터넷의 뉴스그룹이나 음란 사이트(Site)가 접속에 아무런 제한이 없는 상태에서 광범위하게 개설된데다가 청소년의 호기심을 상업적으로 이용하려는 섹스샵(Sex Shop)마저 범람하고 있다.

음란 전자잡지와 기록가능(Writable)한 CD ROM 타이틀이 음란물의 포장지가 되어 값싼 가격에 대량 유통되고, 컴퓨터 통신망을 이용한 전자거래가 음란물의 판매방법으로 악용되면서 정보화 사회를 이루는 최첨단 기술이 청소년의 정서를 극도로 해치고, 성문화의 퇴폐화를 부추기는 수단으로 전락하고 있다.

'96. 1.초 독일 검찰은 미국의 세계적인 BBS인 컴퓨서브(Compuserve)사에 200개 이상의 인터넷 사이트(Internet Site)에 대한 국외접근 차단을 요청하였고, 미국은 통신순화법(CDA: Communication Decency Act)을 제정하여 컴퓨터와 관련한 정보는 물론 영화나 TV 프로그램까지 음란 및 폭력성 정도에 따라 시청등급을 정하도록 의무화하고, TV에 소위, V칩이라는 제한수신장치를 부착하도록 함으로써 정보자유론자들과의 논쟁이 계속되고 있다.

이러한 음란정보에의 접근을 차단하는 기술적인 방법으로는 Net-Nanny, Cyber-Patrol 등 소프트웨어를 이용하여 일정한 용어가 포함된 정보는 전송이 불가능하도록 하는 방법, 전송되는 모든 정보에 대하여 음란정도의 등급을 정하여 공표하는 방법, 그리고 방화벽(Firewall) 방식으로 인터넷에서 음란한 정보를 생산하는 일정한 사이트를 미리 지정함으로써 그에 대한 접속을 차단하는 방법이 있다.

미국 최대의 공중게시판(BBS)인 AOL(America On-Line), 마이크로소프트(Microsoft), 넷스케이프(Netscape) 등 세계 39개의 주요 컴퓨터 통신업체로 구성된 건전정보를 위한 콘서시엄(Consortium)은 청소년들이 인터넷에서의 불건전한 자료에 대한 접근을 차단하기 위하여 업계표준인 PICS(Platform for Internet Selection)에 따라 인터넷의 자료에 대한 등급제를 시행하고, 웹(WWW) 검색 프로그램인 넷스케이프에 청소년이 폭력, 음란물등 불건전자료에 접근할 수 없게 함은 물론, 부모들이 인터넷에 정보를 제공하는 사이트를 등급에 맞추어 선별할 수 있도록 하는 기능을 내장하여 배포하기로 하였다.

19) 상세한 것은 졸저, 전게서, p. 63. 이하 참조.

그러나, 음란서적이나 음화가 제작에서 판매에 이르기까지 엄격한 통제와 함께 엄중한 처벌이 가해지고 있음에도 아랑곳 없이 횡행하는 것을 보면, 위와 같은 차단방법이 과연 청소년들의 음란정보 접속을 차단하는데 얼마나 기여할 것인지는 매우 의문이 아닐 수 없다.

한편, 우리 통신비밀보호법은 일정한 범죄의 수사에 대하여 영장에 의한 감청을 인정하고 있으나, 음란여부나 폭력성의 정도확인 등을 위한 온라인(On-line) 감청은 불허하고 있으므로 수사실무상 커다란 애로가 있는 것이 사실이다.

나. 마약거래, 자금세탁

(1) 의의

암호화한 전자우편과 익명 재전송장치(Anonymous Remailer)[20]를 이용하여 발신인의 전자우편 주소를 은닉할 수 있음을 기화로 수사기관의 추적을 피하여 마약 등 불법거래를 한 다음, 인터넷의 전자화폐를 통한 대금결제로 거래를 완료함으로써 완전범죄를 기도하는 사례도 가능해졌다.

전자화폐는 공개키 암호를 응용한 디지탈 서명제도에 디지캐쉬(Digi-Cash)사를 설립한 암호학자 차움(David Chaum)이 개발한 무색서명기법(Blind Signature Scheme)[21]을 도입하여 거래 상대방의 신원을 노출시키지 않고 금융거래를 가능하게 함으로써 뇌물의 공여, 마약자금의 지급, 조직범죄의 결제자금 등으로 사용되어 자금원에 대한 추적을 불가능하게 한다.

이러한 전자거래는 범죄행위로 인하여 취득한 금전등 재산가치를 은행 등의 금융기관을 통하여 환전, 송금, 예금, 보관위탁하는 방법으로 금전의 출처와 원천을 은폐하거나 금전의 형태를 바꾸어 진정한 소유자를 위장하는 소위, 자금세탁(Money Laundering)의 중요한 수단으로 전락할 가능성이 매우 크다.

(2) 사례

미국 연방상무성의 통계에 의하면 1990년 이후 세계적으로 연간 약 1,000억 내지 3,000억 달러가 범죄행위로 취득되어 자금세탁 과정을 거친다고 한다.

1993년 여름에 호주의 거래자료분석센터(AUSTRAC: Australia Trade Revenue Analysis Center)는 미국의 MITRE사가 미사일 추적 프로그램을 개량하여 연방 수사기관으로 하여금 은행전신환 형태로 은닉된 마약자금의 추적에 사용하게 하려다가 1989년 Bush 행정부의 반대로 시행이 보류되었던 "Screen It"라는 프로그램을 이용하여 북경에 있는 수십개의 은행으로부터 호주에 있는 12개 기업의 예금구좌에 송금되었다가 곧바로 L.A에 있는 동일한 사람의 계좌로 자금이체(EFT: Electronic Fund Transfer)가 계속되고 있는 사실을 발견하였다.

미국과 중국은 오랜동안의 공조수사 끝에 중국계 미국인이 중국의 범죄조직과 연계하여 은행사기, 뇌물, 문서위조 등으로 취득한 1억 5,700만 달러의 자금을 호주를 거쳐 미국으로 송금한 다음, 다시 여러 은행에 분산된 수십 개의 구좌로 "돈 세탁"을 하고 있음을 밝혀냈다.

---

20) 인터넷에서 일정한 사이트(Site)를 경유하여 전자우편을 송신할 경우, 상대방이나 우편을 수취한 사람등 누구에게도 송신인의 전자주소나 인적사항을 특정할만한 자료가 나타나지 않도록 함으로써 전송과정을 추적할 수 없도록 하는 암호학 기술로 David Chaum의 디지탈 혼합이론(Digital Mixes Theory)을 응용한 것이다.

21) 전자화폐로 지정된 전자기록에 대하여 은행이 화폐로 인정하는 디지탈 서명을 한 다음, 상품을 포장하듯이 전자화폐를 포장하여 전자화폐의 사용을 신청한 사용자에게 전송하면, 사용자는 이를 수신하여 포장을 벗기고, 내용물인 전자화폐를 꺼내어 이를 물품대금 지급등 유통에 제공함으로써 최종 소지자가 은행에 결제를 요구할 때에는 당초에 누가 은행으로부터 전자화폐를 수령한 것인지를 알 수 없도록 하여 자금원의 추적을 차단할 수 있도록 하는 암호화기술이다.

(3) 국내의 경우

최근 국내에서도 신용카드가 신용한도액 관계로 여러 개의 카드를 발급받을 수 없고, 부정한 용도에의 사용이 곤란하게 되자 이를 기화로 별도의 예금구좌에 일정금액을 예금한 다음, 동 금액의 한도에서 여러 개의 현금카드를 발행하여 뇌물이나 부정한 거래의 대금으로 사용되고 있다고 한다.

우리나라에서 현재 유통되고 있는 현금카드나 직불카드 등에 앞에서 설명한 무색서명 제도나, 사용카드의 번호가 사용시마다 기록될 수 있는 기능이 내장되었는지는 확인되지는 않았지만, 만약 그러한 기능이 내장되었다는 사실이 일반에 알려진다면 그러한 카드는 쉽게 유통되지 않을 것이 명백하다.

다. 도박

최근 인터넷에 개장된 도박장에서 전자화폐를 이용하여 거금의 도박이 자행되고 있지만, 각국마다 도박에 대한 처벌규정이 다르고, 단속법규가 없는 나라도 있어 전자도박은 급속하게 확산되어 가고 있다.

그러나, 전자도박은 도박을 하고 있는 사람이 누구인지, 연령, 성별, 직업은 물론, 도박에 제공되는 전자화폐가 행위자의 자금인지 다른 사람의 신용카드번호를 훔쳐서 사용하는 것인지를 전혀 모르는 상태에서 행하여질 뿐만 아니라 도박개장자(소위 "House")가 속임수를 쓰더라도 이를 차단할 방법이 없고, 컴퓨터의 오류로 승자에게 도금을 초과배분한다던가, 승자가 없는 것으로 오판하는 경우에 이를 중재할 사람이나 해결할 방법이 없는 등 기능적, 도덕적 폐단이 상존하고 있다.

라. 조세포탈

전자거래중 소프트웨어나 음란자료의 온라인(On-line) 판매등 현물거래를 수반하지 않는 거래행위는 물론, 현물거래를 수반하는 거래도 전자 법률행위에 의하여 행하여지는 경우에는 거래시마다의 추적이 불가능하고, 거래행위 자체는 물론, 소득의 은폐를 감지하기 어려운 까닭에 부가가치세와 같은 간접세이건 소득세와 같은 직접세이거나를 막론하고, 세금징수제도마저 자진신고제로의 전이가 불가피할 전망이다.

특히, 전자화폐를 이용한 대금의 결제는 자금의 추적을 차단할 수 있으므로 장차 전자거래에 대한 적절한 통제나 부정한 거래를 방지하기 위한 별도의 대책이 마련되지 않는다면 이를 이용한 조세포탈은 더욱 극심하여질 것으로 보인다.

마. 각종 위·변조

주차 스티커, 주민등록등본, 특수기관원 신분증의 위조를 비롯하여 수표, 증권, 만원권 지폐의 위조행위가 국내에서도 발생하였다. 장차 고성능 스캐너(Scanner)와 칼라 레이저 프린터(Color Laser Printer)의 보급이 대중화하면 이러한 유형의 범죄는 더욱 증가할 전망이다.

'96. 3.에는 일본의 급진조직인 역군파 대원 다나까 요시미(전중의삼)가 100달러권 미화 수만 달러를 위조하여 전세계에 유통시키다가 검거되었다. 100달러권 위조지폐를 "슈퍼 K"라고 하는데 미국의 컴퓨터범죄 전문수사기관인 U.S.S.S.[22]에 의하면 슈퍼 K는 1990년에 최초로 발견되었으나 1996. 4.까지 북한,이란 등에서 8종류의 위조지폐 10억 달러가 위조되었다고 한다.[23]

22) United States Secret Services: 재무성 비밀수사국

23) 슈퍼 K는 원래 이란에서 제작된 위조지폐기로 제작되었는데 북한이 이란에게 노동, 대포동 등 미사일을 제공하고, 그 대가로 위조지폐기를 취득한 것으로 알려져 있다.

바. 기타

행위자가 누구인지를 쉽게 확인할 수 없고, 다른 사람의 ID를 도용할 수도 있으며, 범행의 흔적을 없애기가 쉽다는 컴퓨터 통신의 특성을 이용하여 다른 사람에 대한 명예훼손이나 모욕, 물품판매를 가장한 사기행위 등도 컴퓨터 통신의 대중화와 더불어 차츰 증가하는 추세이고, 컴퓨터를 이용하여 종래의 전통적 범죄를 범행하려는 기도는 다각적이고, 지능적으로 계속될 전망이다.

1995. 6.에는 서울지검 북부지청에서 화투장에 형광물질을 삽입하여 은닉한 적외선 비디오 카메라(Video Camera)로 이를 읽어들인 다음, 연결된 컴퓨터로 각 패의 승률을 계산하여 승자가 될 수 있는 패의 번호를 도박에 참가한 공범에게 진동기(Beeper: 소위, 삐삐)로 알려주는 고도의 기술을 도입하여 2억 6천만원의 도금을 편취한 사기도박단 3개파 28명이 적발된 일이 있다.

한편, 컴퓨터 통신에서 본인의 확인이나 행위자에 대한 추적이 쉽지않은 점을 이용한 이적표현물의 게시, 반국가단체 또는 이적단체에 대한 고무, 찬양, 동 구성원간이나 적국과의 통신 등 이적행위와 간첩행위도 점차 증가할 것으로 보인다.

제 3 장 정보범죄의 수법과 추세

위와 같은 정보범죄는 컴퓨터범죄의 대표적인 범행수법인 컴퓨터 해킹(Hacking), 컴퓨터 통신과 전화에 대한 도청(Electronic Surveillance), 전화시스템의 교란과 도용(Phone Phreaking)[24], 암호해독(Cryptanalysis 또는, Codebreaking), 컴퓨터 바이러스(Computer Virus)등의 단독 또는 결합적인 형태로 이루어진다.

1. 컴퓨터 해킹

가. 해킹의 의의와 종류

컴퓨터 해킹이란 컴퓨터를 이용하여 다른 사람의 컴퓨터 통신망에 침입하거나 기술적인 방법으로 다른 사람의 컴퓨터가 수행하는 기능이나 전자정보에 함부로 간섭하는 일체의 행위를 가리킨다.[25]

컴퓨터 해킹은 통신망의 운영체제나 소프트웨어의 하자(Bug)를 이용하는 방법과 해킹 프로그램(Hacking Program)을 별도로 제작하는 방법으로 나누어 볼 수 있는데 전자는 CERT, CIAC, Bug-Traq 등 컴퓨터 보안관련기구의 하자보완방법 배포로 점차 감소할 것으로 판단되고, 지능적 방법으로 통신망에 도전하는 후자가 계속 증가할 전망이다.

특히, 패킷 스니퍼링(Packet Sniffering)이나 라우터(Router)의 조작 또는, "ypx"[26]를 이용하여 NIS(Network Information Service)의 활동내역(Map)을 전송받아 써버(Server)를 위조함으로써 권한없는 사람이 시스템에 침입하게 하는 행위, TCP(Transmission Control Protocol) 덤프(Dump)로 TCP 헤더(Header)를 분석함으로써 선두전송번호(ISN; Initial Sequence Number)를 알아내어 시스템간의 핸드쉐이킹(Handshaking)을 방해하거나, 연결하려는 호스트가 전송할 ISN의 SYN 번호를 알아내어 상대방을 위장하는 IP 스푸핑(Internet Protocol

24) 원래는 Phone Freaking이지만, Hacker들의 세계에서는 Phone Phreaking으로 개칭하고 있으므로 본고에서도 같은 단어를 사용하기로 한다. 졸저, 전게서, p. 229.

25) 졸저, 전게서, p.183이하 참조.

26) Network을 통하여 NIS의 Map을 전송하게 하는 응용 프로그램.

Spoofing)[27]으로 보안장치를 뚫고 침입할 수 있게 하는 행위들은 인터넷등 국제적 통신망의 확장과 더불어 크게 경계하여야 할 공격방법들이다.

나. 최근의 동향

(1) 운영체제 자체에 대한 도전

최근 해킹의 동향은 개별적인 시스템에 대한 패스워드(Password)의 분석이나 침입경로에 대한 단순한 탐색이 아니라 보안 프로그램 자체에 대한 도전으로 발전하고 있다.

가령, 윈도우즈(Windows) '95에서 MSPWL32.DLL[28]이 .pwl 화일로 패스워드를 변환하는 과정[29]에서의 하자(Error) 또는, WWW(World Wide Web)의 검색용 프로그램(Navigator)인 넷스케이프에서 CGI 스크립트(Script) 등 "LiveScripts"는 웹페이지(Web Page)의 소유자에게 직접 정보를 전송할 수는 없지만, 자동 로긴 프로그램(Auto Login URL)을 사용하여 곧바로 다른 사람의 스크립트 화일(Script File)에 접속할 수 있는 오류를 이용하는 것이 대표적인 방법이다.

또, 인터넷의 프로그램 언어인 자바 스크립트(Java Script)로 만들어진 실행 프로그램인 자바 애플릿(Java Applet)이 전송을 마칠 때 경로배정을 누락하는 헛점을 이용한 라우팅(Routing)의 조작등은 일반 사용자들도 쉽게 배워 따라할 수 있는 수법들이다.

특히, 비자(VISA)와 마스터카드(Master Card)사가 공동개발하여 '96. 2. 발표한 전자거래의 보안표준인 SET(Secure Electronic Transaction)[30]를 이름없는 프로그래머인 FVH(First Virtual Holdings)사의 보렌스타인(Nathaniel Borenstein)이 불과 한달만에 MS Windows의 API에 내장된 스크린 저장기능(Screen Savers)과 키보드 매크로기능(Keyboard Macros)을 이용한 키보드 해킹으로 보안성을 파괴한 것은 아주 놀라운 해킹사례이다.

(2) 국제적 범행의 증가

컴퓨터범죄의 특성상 당연한 것이기는 하지만, 해킹은 통신망이 연결된 이상 국경을 초월한 국제적인 사건이 되는 경우가 많다. "뻐꾸기의 알(The Cuckoo's Egg)" 사건과, 인터넷 웜(Internet Worm) 사건, 시티은행(CITI Bank) 사건 등이 그것이다.[31]

(가) "뻐꾸기의 알(The Cuckoo's Egg)" 사건

"뻐꾸기의 알" 사건은 1987년 초부터 1988년 7.경까지 독일의 하노바(Hanover)에 있는 Marcus Hess 등 5명의 해커들이 브레멘(Brehmen) 대학의 인터넷 계정으로 Datex-P 통신망에 침입한 다음, 대서양에 떠있는 Wester III, Comsat 인공위성을 통하여 간첩행위를 하다가 적발된 사건이다.

이들은 국제 게이트웨이(Gateway)[32]인 팀넷(Tymnnet)를 거쳐 클리포드 스톨(Clifford

27) 국내에서 발생한 컴퓨터 해킹사고중 가장 기술적인 것으로 일컬어지는 한국과학기술원 학생들의 포항공대 컴퓨터에 대한 해킹사건에도 IP Spoofing을 이용하여 상대방의 관리자(Root)디렉토리에 있는 .rhost 화일로 계정을 취득하여 범행한 것으로 밝혀졌다.

28) Microsoft Password Language Dynamic Linker.

29) 40비트의 스트림암호인 RC-4를 이용하는 방법이었지만, XOR을 하는 라운드마다 같은 수치가 계속 입력되는 하자가 있어 이를 알아낸 해커가 패스워드 화일을 해독하였다.

30) 신용카드와 스마트카드, 전자화폐등 전자거래의 표준으로 사용하기 위하여 만든 암호화 기술로서 마스터카드사가 IBM, NETSCAPE, GTE, CyderCash 등과 협력하에 제작한 SEPP(Security Electronic Payment Protocol)와 비자카드사가 마이크로소프트와 공동으로 개발한 STT(Secure Transaction Technology)를 결합한 것이다.

31) 상세한 것은 졸저, 전게서, p.216 이하 참조.

32) 통신망 마다 다른 문자와 기호체제를 재구성하여 통신이 가능하도록 중개하는 별도의 통신망

Stoll)이라는 천문학자가 근무하는 캘리포니아의 로렌스 버클리(Lawrence Berkeley) 연구소와 접속이 가능한 미국의 군사용 컴퓨터 통신망인 Arpanet[33]과 Milnet[34]에 연결된 중요 군사시설의 컴퓨터에 침입한 다음, 각종의 군사기밀을 탐지하여 K.G.B.에 양도하고 그 대가로 마약을 받아오다가 위 천문학자의 추적으로 검거되었다.

(나) 인터넷 웜(Internet Worm) 사건

"인터넷 웜" 사건이란 1988. 11. 인터넷에 자기복제 기능을 가진 프로그램이 침투하여 15시간 동안 썬 원크스테이션(Sun Worksation) 등 UNIX를 운영체제로 하는 컴퓨터와 Internet에 연결된 미국 전역의 2,000여대의 컴퓨터에 전파됨으로써 컴퓨터 속도를 저하시키거나 시스템을 정지시킨 사건이다.

Purdue 대학의 스패포드(Eugine H. Spafford)와 Massachusetts 대학의 에이친(Mark W. Eichin) 등은 위 Worm이 버클리(Berkeley) 계열의 UNIX 컴퓨터에만 감염된다는 점과 동 프로그램에 "RTM"이라는 작성자의 이름이 기재된 것을 기초로 하여 범인을 검거하였는데 동인은 코넬(Cornell) 대학의 Robert T. Morris라는 대학원생인데다가 UNIX의 암호함수인 crypt()를 만들어낸 Bob Morris의 아들이라는 점에서 큰 충격을 주었다.

(다) 시티은행(CITI Bank) 사건

"시티은행" 사건은 1994. 8. 이스라엘 경찰이 위조려권을 소지하고, 시티뱅크 은행의 알젠틴 지점으로부터 이스라엘 은행으로 전자송금된 백만달러 가량을 인출하려던 러시아인을 검거함으로써 동 은행의 전자결제 시스템은 물론, 세계 유수은행들의 전자결제 콘서시엄인 SWIFT (Society for Worldwide Interbank Financial Telecommunication)의 전산망까지 조작하는 조직이 있다는 사실이 드러난 사건이다.

미국, 러시아, 이스라엘 등 관련국가들이 국제공조수사를 계속한 결과, 러시아에 있는 성페터스부르그 대학의 대학원생인 블라디미르 레빈(Vladimir Levin)등 30여명이 은행간의 네트워크(Network)에 관하여 공부하다가 범행을 모의한 나머지, 시티뱅크의 알젠틴과 인도네시아 지점들로부터 1,000만 달러 이상을 빼내어 미국, 이스라엘, 네덜란드, 독일, 핀란드 등 여러나라의 금융기관으로 분산한 다음, 자금세탁을 하여 온 사실이 밝혀졌다.

(라) 세가의 해커 Mitnick

1993. 5. 북한의 핵문제로 세계가 시끄러울 때 16세의 영국인 소년이 미 국방성의 Arpanet에 침입하여 미국의 탄도 미사일, 전투기의 설계 등에 관한 화일들을 Internet의 공개 Forum에 올려놓았던 사건이나 미국의 악명높은 Hacker로서 Internet의 주요한 호스트 컴퓨터(Host Computer)들에 침입하여 해킹을 감행한 미트닉(Kevin David Mitnick) 사건도 대표적인 해킹사건의 하나이다.

특히, 미트닉은 모든 수사기관이 오랜동안 추적해오던 끝에 FBI가 일본계의 컴퓨터 전문가인 시모무라(Tsutomu Shimomura)와 함께 검거하였는데 미트닉[36]은 1995. 4.에 발표되어 세계적인 파문을 일으킨 단 파머(Dan Farmer)의 컴퓨터 통신망에 대한 보안점검 프로그램인 SATAN(Security Administrator Tool for Analyzing Networks)을 해킹, 폰 프리킹, 도청 등 갖가지 컴퓨터범죄에 이용하였다고 한다.[36]

33) 미국 고등방위연구소 전산망(Defence Advanced Research Projects Agency Network)
34) 미국 군사정보통신망으로 Arpanet와 연결되어 있다.
35) 동인은 법정형을 경합범으로 의율할 경우 징역 460년을 선고받을 수도 있다고 한다.
36) Internet Forum, Risks-l, risks16.90, 1995. 4., 뉴욕타임즈, 1995. 3.11, p.30, 참조, '96. 2. Tsutomu Shimomura가 뉴욕타임즈의 기자인 John Marcoff와 함께 Kevin Mitnick의 추적과 검거에 관하여 "Takedown"이라는 책을 발간하였다.

(3) 국내의 경우

국내에서도 1995. 8. 한국통신의 인터넷 서비스망인 KORNET과 민간업체인 나우콤의 나우누리에 해커가 침입하여 중요자료를 삭제하거나 서울대 등 여러 대학과 연구소의 통신망을 교란한 사건이 발생하였다.

또, 미국의 INFONET, MCI등의 ESS (Electronic Switching System: 전자교환기)를 거쳐서 한국데이터통신(DACOM)의 ISDN (Integrated Services Digital Network: 종합정보통신망)에 침입한 뒤, 선경이 운영하는 BBS의 NUA(국제 데이터통신 고유번호)로 미국의 AT&T와 프랑스 TRANSPAC의 ESS를 경유하여 남파리대학 수학연구소에 잠입한 다음, 화일변경을 행한 사건이 언론에 보도되기도 하였다.

다. 전망

윈도우즈(Windows) '95가 네트워킹(Networking)을 기본으로 제공함으로써 대학이나 연구소, 정부기관, 대기업 등 대형 컴퓨터를 사용하는 곳이 아닌 개인용 컴퓨터에서도 인터넷과의 결합등 네트워크의 구축이나 시스템의 개방이 가능해짐에 따라 해커들의 활동은 네트워크에 연결된 개인용 컴퓨터까지 더욱 치밀하고, 깊숙하게 침투할 전망이다.

2. 폰 프리킹(Phone Phreaking)

가. 의의

폰 프리킹은 전화교환기가 전자식으로 전환되면서 UNIX기종의 컴퓨터를 이용하게 되자 컴퓨터 해킹을 통하여 전화시스템을 교란하거나 전화기의 요금계산에 관한 기본원리를 악용하여 전화를 도용하는 행위이다.

나. 전화시스템의 교란

전화시스템의 교란방법으로는 컴퓨터 해킹을 통하여 전화교환 시스템을 운영하는 컴퓨터에 장애를 초래하는 방법 외에도 ESS의 실험실(Master Control Center)에 침입하여 전화교환 프로그램을 변경하거나, 중계교환(Toll Transit Switch)의 연동을 차단하는 행위, 사용자가 다이얼한 번호가 아닌 다른 번호로 연결되게 하는 착신통화전환(Call-forward Another Number) 행위, 전화료금 계산프로그램을 조작하는 행위, 가입자선(Local Loop)신호, 감시신호, 선택신호 등에 사용되는 신호방식의 작동을 변경하는 행위, 패킷(Packet)망의 전송장치(STP: Signal Transfer Points)나 서비스 제어장치(SCP: Service Control Points)에 침입하여 패킷전송을 조작하거나 방해하는 행위, 의사 난수발생기(PRNG: Pseudo Random Number Generator)를 이용한 음성 스크램블(Voice Scramble)[37] 루틴을 차단하여 음성비화를 방해하는 행위 등을 예로 들 수 있다.[38]

다. 전화의 무단사용

Black Box, Blue Box, Beige Box, Red Box 등 전화기의 원리를 이용한 각종 Color Box의 사용, 루프(Loop, 환선 또는 측선)의 이용, 위조,변조한 전화카드의 사용, 대표전화(PBX Line Hunting Service), 구내 자동착신전화(DID: Direct in Dialing) 제도를 이용하여 외부에서 대표전화로 전화한 뒤 구내 사용자로

37) 음성신호를 여러개의 주파수 성분 또는 시간성분으로 나눈후 의사난수 발생기를 이용하여 각 요소를 변형 또는 자리바꿈함으로써 도청자가 그 내용을 알아낼 수 없도록 하는 기법.

38) 상세한 것은 졸저, 전게서, p.261 이하 참조.

위장하여 장거리전화나 국제전화를 함부로 사용하는 다이버팅(Diverting), 음성사서함(VMB: Voice Mail Box)이나 휴대용 전화(Cellular Phone)의 도용, 패킷망의 무단사용등이 주요한 범행수법이다.[39]

라. 사례

(1) 전화시스템의 교란

1990. 1.15. AT&T 사의 장거리 전화교환 시스템이 작동되지 않아 가입자 수만명의 전화가 불통되고, 1991. 7.에는 Bell Atlantic사와 Pacific Bell사의 전화교환 시스템이 뒤엉켜 2일 가까이 1,200만명의 가입자가 전화사용을 할 수 없게 된 사건이 발생하였다.

두 사건은 모두 프로그램의 오류인 것으로 발표되었지만, 이러한 통신대란이 Phone Phreaking에 의하여 발생할 가능성은 충분하다.

우리나라에서도 '94. 10.경 서울의 일부 전화국에서 전화료금 프로그램이 잘못 조작되어 가입자들에게 전화료금이 잘못 부과된 일이 있었고, '96. 4.에는 남인천전화국의 전용회선 24,000여선이 회선운용 프로그램의 이상으로 완전마비된 일도 있었지만, 범죄행위에 의한 것인지는 밝혀지지 않았다.

(2) 착신통화전환(Call-forward Another Number)

또, 미국에서는 1989. 6. 유명한 해커그룹인 LoD(Legion of Doom)의 16세 소년이 플로리다(Florida)에 있는 벨사우스(Bell South) 전화국의 프로그램을 변경하여 주립 보호관찰소에 전화를 걸면 뉴욕에 있는 폰 섹스업소로 연결이 되도록 착신통화전환을 함으로써 젊은이들에게 시내전화 요금으로 신나는(?) 모험의 기회를 주었던 일이 있었다고 한다.

이러한 방법은 112나 119 등 긴급전화 시스템에 대하여 시도될 경우에는 국가적 또는 사회적으로 심각한 문제를 야기할 수도 있다.

(3) 다이버팅(Diverting)

1994. 11. 캐나다의 퀘벡(Quebec)지역에서는 1993. 8.부터 1994. 3. 사이에 12명의 프리커들이 미국 펜실바니아(Pensylvania)의 센토코(Centocor) 제약회사의 대표전화(PBX)를 1,600번이나 무단사용하여 50,000달러 상당의 전화료금을 면탈하다가 적발된 일이 있다.

(4) 휴대용 전화(Cellular Phone)의 도용

휴대폰은 보통 수신인에게 두자리 수의 전화번호와 함께 발신인의 휴대폰에 하드웨어(Hardware)적으로 등록된 일련번호를 전송하게 되는데 이러한 번호들은 암호화되지 아니한 상태에서 전송되므로 이를 수신하여 휴대폰을 복제한다.

휴대폰의 도용은 미국에서 마약거래자들이 수사기관의 추적을 차단하기 위하여, 또는 이민사회에서 국제전화나 장거리 전화를 사용하는데 주로 사용되다가 중산층에까지 폭넓게 확산되기에 이르렀는데 '94년에는 이러한 유형의 휴대폰 남용으로 약 2억불이상의 전화료금이 면제되거나 다른 사람에게 청구되었다고 한다.

국내에서도 1995. 9. 서울지검 북부지청이 휴대폰의 EEPROM에 등록된 헥사번호를 헥사조정기로 복제하여 다른 사람의 전화번호를 이용할 수 있도록 하는 휴대폰번호 복제단을 일망타진한 일이 있다.

39) 상세한 것은 졸저, 전게서, p.252 이하 참조.

3. 암호해독

가. 암호해독의 중요성

2차대전 당시 롬멜이 북아프리카에서 용맹을 떨친데는 정예화된 독일 기갑부대를 종횡무진하게 지휘한 롬멜의 기지도 있었지만, 카이로 주재 미국 대사관의 암호송신을 해독한 독일군의 암호해독술이 크게 기여하였다고 한다.

또, 미군이 일본군의 암호를 해독함으로써 "식수가 부족하다"는 일본의 공격명령 암호를 송신하는 역공작을 통하여 미드웨이(Midway) 해전을 사전에 감지하거나, 일본의 연합함대 사령관인 야마모도가 북 솔로몬제도를 시찰하려던 계획을 간파하여 그가 탑승한 비행기를 격추함으로써 2차대전을 승리로 이끌었던 일은 일반인들에게도 잘 알려진 사실이다.

암호는 원래 국가의 비밀을 보안할 목적으로 군사, 외교분야에서 사용되기 시작하였지만, 금융기관들의 전자자금이동(EFT: Electronic Funds Transfer)에 널리 사용되면서 경제, 금융분야에서 확고한 자리를 잡은 이래, 통신 시스템이나 특정한 보안시설, 중요한 비밀장치 등에 대한 사용,출입이 승인된 사람을 확인하기 위한 동일성의 인증(Authentication), 암호화 키에 대한 관리(Key Management), 디지탈 서명(Digital Signature), 신원확인(Identity Verification)에 널리 이용되는등 광범위한 응용분야가 개척되고, 오늘날에는 개인이나 기업간의 통신에 이르기까지 보편적으로 사용되고 있다.[40]

특히, 컴퓨터 통신에 대한 도청기술이 급속히 발전함에 따라 개인이나 기업들에게는 프라이버시나 산업비밀을 지키기 위한 간편한 암호화 기법의 필요성이 높아지면서 암호화 기법은 사회생활의 각 분야에 걸쳐 다양하게 이용되기에 이르렀다.

그러나, 암호제도의 유용성을 알게된 범죄집단이나 범죄자들도 그들의 통신에 암호를 사용함으로써 범인을 검거하거나 증거자료를 수집하는 과정에서 물리적인 증거물을 확보하더라도 암호화된 증거를 해독하지 못할 경우 범인에게 형사제재를 가할 수 없을 수도 있으므로 암호제도는 공공의 안녕과 사회방위에 커다란 위협의 대상으로도 등장하였다.

마치, 가진 자들만의 질서정연한 운행으로 시작되었던 자동차문화가 대중화를 거듭하면서 교통법규가 생기고, 특정한 경우에는 교통지옥으로 변하여 거리질서가 마비되듯이 암호화 기법도 같은 길을 걷게 된 것이라고 할 수 있다.

나. 범행수법

(1) 의의

암호해독은 해독키의 관리소홀, 비밀번호의 예측가능성, 모니터의 방사현상, 통신망의 키보드 입력에 대한 모니터링(Monitoring) 등으로도 가능하지만, 여기서 암호해독이라 함은 해독행위자가 암호문만을 가지고 평문에 대한 해독을 감행하는 방법(소위, 무작정 공격: Bruteforce Attack)이 아니라 평문의 암호화에 사용된 알고리즘(Algorithm)의 종류, 사용된 운영체제등 시스템에 대한 모든 정보를 알고 있는 상태에서 암호화에 사용된 키만 모르는 경우에 그 키를 찾아내어 암호문을 평문으로 해독하려는 행위를 지칭한다.

(2) 공격방법의 종류

암호를 해독하는 기술로는 단순 암호문공격, 지실평문공격, 선택평문공격, 최적선택 평

40) 상세한 것은 졸저, 전게서, p.271 이하 참조.

문공격, 선택 암호문공격, 시간공격 등의 방법이 있다.

첫째, 단순 암호문공격(Ciphertext Only Attack)은 취득한 암호문만을 이용하여 상대방의 신상이나 주변상황, 발생가능한 현실 등을 추측함으로써 예상되는 평문을 대입하여 평문을 취득하는 기술이지만, 해독가능성은 매우 낮다.

둘째, 지실평문공격(Known Plaintext Attack)은 암호문을 통신한 당사자들로부터 입수한 많은 암호문과 평문의 조합들로부터 암호문의 생산에 사용되었던 키를 찾아 다른 암호문으로부터 평문을 해독하려는 기술이다.

셋째, 선택평문공격(Chosen Plaintext Attack)은 취득한 평문을 골라서 암호화 알고리즘에 입력하여 출력을 확인함으로써 사용된 키를 찾아내는 방법이다.

넷째, 최적선택 평문공격(Adaptively Chosen Plaintext Attack)은 출력된 암호문을 확인하면서 평문을 선택하여 입력하면서 사용된 키를 확인하는 기술이다.

다섯째, 선택 암호문공격(Chosen Ciphertext Attack)은 대칭키 암호를 사용한 암호문에서는 불가능하고, 공개키 암호를 이용한 암호문에서만 가능한 방법으로 암호문을 골라서 입력하고 이에 해당하는 출력을 확인하여 사용된 키를 추적하는 방법이다.

여섯째, 시간차 공격(Timing Attack)은 Paul Kocher가 1994. 10.에 개발한 공개키 암호에 대한 해독방법으로서 평문이 암호화되는데 필요한 시간차를 100만분의 1초 단위로 분석함으로써 평문을 추적하는 방법이다.

이 방법은 그 파급효과가 대단히 큰 것으로 알려졌으나, 개발자가 공격방법에 관한 개요를 공표하면서 구체적 이론까지 곧 공개하기로 하였는데 1년이 넘도록 구체적 내용을 공개하지 않아 일부 해커그룹에서는 개발자가 NSA(National Security Agency: 미국 국가안전국)에 포섭당하였을 것이라는 풍문마저 돌고 있다.[11]

그러나, 위와 같은 암호해독법보다 훨씬 더 효과적이고 위력적인 것은 뇌물공여에 의한 키의 매수(Purchase-Key Attack)를 포함하여 협박, 공갈, 고문 등에 의한 키의 획득방법을 총칭하는 고무호스 암호분석(Rubber-Hose Cryptanalysis)이다.

(3) PGP(Pretty Good Privacy)[42]의 경우

PGP를 사용한 전자우편은 일반적으로 보안이 완벽한 것으로 알려져 있다. 그러나, 해커들 중의 일부는 PGP도 2.0이하의 버전들은 안전하지만, 버전 2.1 이후의 것들에 대하여는 NSA가 Novell, Microsoft, Borland, AT&T 등 컴파일러 제조업자로 하여금 컴파일 과정에서 PGP를 조작하여 쪽문 만들기(Trap Doors)를 장치하도록 하였기 때문에 PGP로 암호화된 전자우편을 해독할 수 있다고 주장한다.

해커들은 GNU[13]의 2.2.3 버전 이후 GCC 컴파일러로 PGP 버전 2.1.이후의 소스코드(Source Code)를 컴파일한 PGP로 암호화한 전자우편은 NSA, FBI, CIA나 MJ12 등의 정부기관들이 해독하고 있다고 주장하는데 1995.

11) 이에 대하여 Saso Tomazic 같은 학자는 Timing Attack은 암호화 과정에 소요되는 정확한 시간을 측정한다는 것은 차라리 다른 사람의 컴퓨터에 있는 평문이나 암호화키, 패스워드를 알아내는 것보다도 어렵고, 이러한 공격방법에 대하여는 암호화 수행시간이 암호화 키와 무관하도록 알고리즘을 쉽게 변경할 수 있다고 주장한다. Kocher,103 참조.

12) Pretty Good Privacy, Philip R. Zimmerman이 스위스의 Xuejia Lai와 James Massey가 창안한 IDEA(International Data Encryption Algorithm)와 공개키(Public-key) 알고리즘을 이용하여 개발한 전자메일의 암호화 기술.

13) Gnu is Not Unix의 약자.

2. 아이다호(Idaho)에서 좌익운동가인 슈타인골트(Craig Steingold)가 검거될 당시 동인이 PGP로 전송한 전자우편을 해독한 사본을 경찰이 소지한 것을 그 증거로 들고 있다.

그들은 1992년에 체포된 PGP의 제작자 짐 머만(Philip Zimmerman)이 NSA로부터 불기소처분을 담보로 버전 2.1이후의 PGP에 대하여 추적이나 적발이 불가능한 쪽문만들기 방법을 포함하도록 강요받았을 것이라고 주장하고 있다.[44]

다. 암호해독의 동향

암호해독을 이용한 정보범죄는 통신망 사용자에 대한 인증절차를 위하여 설정 또는 지정된 토큰(Token)이나 개인식별번호(PIN)[45]의 설치,지정에 사용되는 암호화 알고리즘을 해제하거나 사용자의 식별코드(ID)와 계정관리(Account Administration), 전자지갑이나 전자화폐(Electronic Cash, Digital Money) 또는 각종 통신망에서의 인증절차를 위한 디지탈 서명에 사용되는 암호를 해독하는 행위가 그 대표적인 사례이다.

그리고, 클라이언트 서버 프로세스(Client/Server Process)에 대한 세션계층(Session Layer)의 암호화 절차를 해제하거나, 중요한 데이터의 차단과 재생을 방지하기 위한 일련번호 처리장치와 수신확인을 위한 암호화 조치를 무용화하는 행위, 디지탈 서명의 위조, DES, PGP, PEM 등으로 암호화된 전자문서나 전자우편의 해독을 통한 비밀침해, 스마트카드나 VOD(Video On Demand), CATV 등의 한정수신 시스템에 대한 스크램블러의 해독등도 최근에 행하여지는 중요한 암호해독행위에 속한다.

1995. 9.에는 넷스케이프(Netscape)의 암호화 프로토콜 기술인 SSL(Secure Socket Layer)에 사용된 40비트의 RC-4 스트림 암호(Stream Cipher)[46]를 해독하여 다른 사람의 신용카드번호등을 수집하는 수법이 공표됨으로써 새로운 보안기법이 강구되었고, 어떤 해커는 PGP의 경우도 해독이 가능하다고 공표하는등 암호와의 전쟁은 더욱 지속될 전망이다.[47]

라. 암호의 응용과 정보범죄

(1) 전자화폐

전자화폐 제도는 은행잔고가 있는 사용자가 거래은행의 인증이 되지 아니한 전자화폐에 자신의 디지탈 서명을 한 뒤 은행의 컴퓨터에 송부하면, 은행은 본인임을 확인하여 은행의 디지탈 서명으로 인증을 한 뒤 사용자의 컴퓨터에 전송하고, 이를 수신한 사용자는 자신이 대금을 결제하여야할 상대방의 컴퓨터로 전송하면 상대방은 전송된 전자화폐를 인증한 은행에 조회함으로써 정상적인 전자화폐로 인정될 경우에는 대금으로 수령하여 자신의 거래은행에 예금하거나 다른 전자거래에 사용할 수 있도록 하는 제도이다.[48]

---

44) Erik Bloodaxe(Chris Goggans) 등, Phrack Magazine, Vol. 4, Iss. 47,, 1995. 4.

45) Personal Identification Number : 신용카드, 전화의 Calling Card제도 등에서 사용이 허용된 사람에게만 고유로 부여하는 개인식별번호.

46) Ron's Code

47) Raph Levien은 PGP Key에 대한 공격을 통하여 실제로 PGP의 창시자 Phil Zimmermann이 1992. 7.에 만든 1,024비트의 키를 위조할 수 있음을 증명하였다. ATTACK.PGP 참조.

48) 우리나라 은행법은 예금의 수입 등 금융기관의 은행업은 금융통화위원회의 인가없이 영위할 수 없고(동법 제38조의 2. 제3조 제1항), 외국환의 경우, 대외지급수단의 매매,발행등 환전업무는 재정경제원 장관의 인가를 받아야 하므로(외국환관리법 제7조 제1항, 제9조 제1항) 은행이 아닌 개인의 전자화폐의 유통기관개설은 동법들의 규제에 의하여 현재로서는 매우 어려운 형편이다.

1995. 7.부터 영국의 스윈던(Swindon) 시에서는 먼덱스 전자화폐(Mondex E-cash)사가 스마트카드 형태의 전자지갑을 이용하여 모든 거래에 전자화폐를 이용할 수 있도록 하였고, 같은해 11.에 미국 세인트루이스의 마크 트웨인(Mark Twain) 은행이 디지캐시(Digital Cach) 기술을 응용하여 계좌를 개설한 고객이 자신의 예금을 직접 자기 컴퓨터에 입금할 수 있는 전자화폐 서비스를 제공함으로써 인터넷에서는 이를 이용한 물품거래와 전자도박 등이 횡행하고 있는데 앞으로 모든 분야에서 전자지갑과 전자화폐를 이용한 거래가 활발하여질 것으로 보인다[49].

(2) 전자문서

전자문서는 다양한 통신망을 기초로 교환되는 개체간의 정보를 사람의 중재없이 독립된 컴퓨터 프로그램간에 관리, 교환하는 EDI (Electronic Data Interchange)와 같은 전자식 시스템에서 표준화된 양식과 코드체계를 이용할 수 있도록 합의한 정형적 양식의 표준이다.[50]

현행법상 무역업무 자동화촉진에 관한 법률[51]과 공업 및 에너지 기술기반조성에 관한 법률,[52] 화물유통촉진법[53]에서 동 업무들과 관련한 전자문서에 한하여 문서성을 인정하고, 개정된 전산망 보급확장과 이용촉진에 관한 법률[54]도 당국이 고시하는 인,허가절차 등에 관한 전자문서에만 문서성을 인정하고 있다.

그러나, 장차 디지탈 서명을 이용한 스마트카드 사용이 일반화되고, 전자문서의 다양한 활용과 전자우편의 일상화 등 전자 법률행위가 보편화될 경우, 암호화된 전자문서나 전자우편의 내용을 해독하거나 디지탈 서명의 위조행위 등 암호의 해독이 비밀침해의 수단으로 중대한 역기능을 초래할 것이 분명하다.

4. 도청

가. 도청의 의의

도청은 다른 사람의 통신에 간섭하여 통신중에 있는 정보의 내용을 함부로 수신하는 행위를 가리킨다.

과학기술의 발전과 함께 최첨단 도청장비가 속출하여 개인의 프라이버시와 통신망의 안전에 중대한 위협이 되었고, 한편, 국가기관이 범죄인들의 통신을 합법적으로 감청하여 증거자료로 활용하여야 할 필요성이 점차 커져가고 있으므로[55] 외국에서는 오래전부터 전자 감시학(Electronic Surveillance)라는 이름으로 학문적 고찰이 계속되어 왔다.[56]

나. 도청의 종류

도청에는 음성에 대한 도청과 비음성정보에 대한 도청이 있다.

음성에 대한 도청은 전화도청(Wiretapping) 외에 패러볼릭 마이크(Parabolic Microphone), 무선송신기(Radio Transmitter), 광학 발신기

49) VISA카드회사는 SVC(Stored Value Card)라는 이름으로 Smart Card형태의 전자지갑을 개발하여 위 몬덱스를 비롯한 미국, 덴마크, 벨기에, 핀란드 등 20개국에서 시행을 추진하고 있으며, 우리나라에서도 '95. 9.부터 동남은행을 비롯한 28개 시중은행이 이 형태의 전자지갑 거래를 추진하고 있다.

50) 이필중,전윤호, "EDI 표준과 관련된 보안서비스에 관한 고찰" 통신정보보호학회지, 제4권 제2호, 한국통신정보보호학회, 1994. 6. p.59.

51) 동법 제2조 제7호.

52) 동법 제8조 제1항, 제2항.

53) 동법 제2조 제11호.

54) 동법 제2조 제3호.

55) Willam B. Moran, Covert Surveillance and Electronic Penetration, Lumpanics Unlimited, 1983., pp. 32-33.

56) Office of Technology Assessment, Electronic Surveillance and Civil Liberties, Congress of the U.S., 1989., pp. 9-10.

(Optical System) 등의 장비 또는 음성자극 스위치(Voice Actuation Switching Devices) 등을 첨부한 고성능 녹음기에 의한 도청(Audio Eavesdropping)으로 행하여지는 것이 보통이고, 비음성정보에 대한 도청은 주로 무선전신(Teletype), 텔렉스(Telex), 팩시밀리(Faximilie) 등 문자의 송,수신등 통신자료에 대한 도청과 무선으로 송신되는 이동통신에 대한 무선도청, 컴퓨터 네트워크에 대한 도청 등으로 행하여지고 있다.[57]

다. 컴퓨터 통신에 대한 도청

컴퓨터 통신에 대한 도청은 컴퓨터를 연결하는 케이블이나 전화선 또는 마이크로웨이브(Microwave) 등 무선에 대한 간섭으로 이루어진다.[58]

1985년 네덜란드의 Wim van Eck는 TV 수상기와 같이 매우 큰 전자파를 수신하는 설비 주변에서 컴퓨터를 작동하면 컴퓨터와 연결되어 있지 않더라도 TV 화면이 컴퓨터 모니터(Monitor)의 역할을 한다는 전기 전자파 방사현상(van Eck Radiations)을 발견하였다.

그 이후 위와 같은 현상을 이용한 TEMPEST(Transient Electromagnetic Pulse Standard)[59] 모니터링에 의한 추적기술은 감청령장의 집행은 물론, 국가정보기관의 정보수집, 경쟁기업간의 산업 스파이, 노동조합에 대한 감시 등에 이용되고 있는 것으로 알려지고 있다.

"반 에크 방사현상"은 공기중에서 뿐만 아니라 전선, 수도관, 스프링쿨러 등에서도 같은 결과가 발생하므로 1991년에는 동 현상을 이용하여 미국의 어느 현금자동인출기(ATM) 회사의 메인 컴퓨터를 조작하여 현금카드의 자료를 변경하는 시범이 Hacker들의 모임에서 시연(?)되기도 하였고, 1992년 가을에는 Chemical 은행 등 뉴욕의 주요은행들에 위와 같은 장비를 이용하기 위하여 설치된 안테나들이 다수 발견되었다.[60]

1995. 초에는 미국의 한 Phreaker가 광섬유에서 장곡효과[61]를 발생하게 하여 광 케이블에 대한 도청까지 가능하게 되었으므로 암호화 체계가 완비되지 아니한 개인이나 기업들간의 통신에 대한 침해가능성이 매우 높다.

컴퓨터 통신에 대한 도청은 컴퓨터 사용감시기(Computer Usage Monitor), 전자우편 감시기(Electronic Mail Monitor or Interception), 위성전파 감시기(Satellite Beam Interception) 등을 이용함으로써 도청가능 영역이 광범위해지고, 이동도청까지 가능하게 되었다.

라. 음성, 영상정보에 대한 도시청

음성정보를 스크램블링(Scrambling)하는 방법에는 시간령역에 대한 스크램블링과 주파수 영역에 대한 스크램블링이 있다.

그러나, 시간령역에 대한 스크램블링은 도청한 신호에 가능한 모든 키를 대입하여 역 치환 과정을 수행한 다음, 영교차율(Zero-Crossing)[62]을 비교함으로써 의사난수 치환법, 유니폼 치환법 또는, 의사난수-유니폼 치환법으로 비화시킨 모든 경우에 대하여 해독이 가능하고, 주파수 영역에 대한 스크램블링은 도청한 신호를 FFT(Fast Fourier Transform)[63] 변환한 다음,

57) 상세한 것은 졸저, 전게서, p.374 이하 참조.
58) Willam B. Moran, 전게서, pp.94-96., 99-100.
59) 구체적인 기준은 NSA가 비밀로 분류한 NACSIM 5100A에 기록되었다. HACK,318 참조.
60) Winn Schwartau, 전게서, pp.142-144.
61) Macrobending Effect: 광섬유에 일정한 자장을 유도하여 전송되는 빛을 180도 회전하게 하는 방법.
62) 신호파형이 크기가 영(zero)인 점을 지나는 횟수를 나타내며 신호파형이 시간축을 지나는 모든 경우에 발생한다.
63) 고속 퓨리에 변환: 삼각함수의 주기성을 이용하여 데이터의 순서를 바꿈으로써 시간이 걸리는 나눗셈의 횟수를 대폭 감소시키는 방법으로 데이터 수열에 대한 퓨리에 변환을 고속으로 실행하는 계산방법이다.

비화된 신호의 주파수 대역을 역치환하여 위상 판별을 행함으로써 해독이 가능해진다.

최근에 정보화 사회의 첨단 기술로 대중들에게 점차 유료로 공개되고 있는 CATV나 VOD (Video On Demand)등 한정수신 시스템(Conditional Access System)에 대한 도시청방법도 점차 지능화되어가고 있다.

일반적으로 TV영상에 대한 스크램블링 방식으로는 주사선 교환방식(Line Permutation)과 주사선 회전방식(Line Rotation)이 있으나, 스크램블링 방식에 대한 알고리즘이 한정되어 디스크램블러(Disscrambler)의 제작도 용이하고, 제작비용도 작게 소요되어 외국에서는 공공연히 판매되고 있는 실정이다.

마. 사례

미국이 월남전에 사용한 컴퓨터들을 종전후에 확인한 결과, 컴퓨터의 CPU에 소형 무선송신기가 은닉되어 원거리에서 컴퓨터의 통신내역을 그대로 도청할 수 있도록 된 사례가 다수 발생하였다고 보도된 바 있다.[64]

박동선사건과 관련하여 미국 CIA의 청와대 도청사건이 세간을 시끄럽게 하였고, 최근에는 미국 국가안전국(NSA)이나 캐나다의 통신보안국(CSE)이 한국을 비롯한 미국주재 외국대사관이나, 외국 국가원수의 집무실까지 도청하였으며, CIA가 미.일간의 무역협상에서 일본측을 도청하였다는 사실이 보도되어 큰 충격을 주었다.

우리나라 고속철도 수주와 관련하여 독일의 ICE가 프랑스의 TGV를 이겨내지 못한 것은 프랑스 첩보기관이 독일의 판매정보를 도청하였기 때문이라는 주장도 있다.

바. 전망

개인의 사생활은 물론, 산업정보, 국가안보에 관한 정보들이 최첨단의 장비에 의하여 은밀하고, 조직적으로 도청되고 있는데 특히, 냉전시대가 끝나고, 군사무기의 경제무기화가 급진전되면서 인공위성을 이용한 영상확대장치와 결합된 국가적 차원의 도청까지 감행될 가능성마저 배제할 수 없다.

'95. 10. 러시아에서 인질로 잡혔던 현대전자 직원들을 구출하는데 최신의 도청장치가 큰 공헌을 한 것처럼 도청이 유용하게 사용되는 경우도 있지만, 전화번호만 알면 도청이 가능한 핸드폰, 팩시밀리 도청기, 무선 비디오 송신기, 일단 설치하면 세계 어디서나 수신이 가능한 원격 도청장비, 레이저를 사용하여 도청대상장소에 별도의 장치가 필요없어 적발가능성이 거의 없는 레이저도청기 등 첨단장비가 계속 개발되고, 위성통신과 이동통신의 발전, 무선 데이터통신(Wireless Data Networking)과의 결합으로 우리의 기본권을 침해하는 도청은 더욱 기승을 부릴 전망이다.

5. 컴퓨터 바이러스(Computer Virus)

가. 의의

컴퓨터 바이러스란 다른 컴퓨터 프로그램 또는 사용자가 실행할 수 있는 전자기록의 집합, 예컨대 오버레이 화일(Overlay File), 장치구동기(Device Driver), 운영체제(Operating System), 부팅에 필요한 데이터(Boot Record) 등에 자신 또는 그 변형을 복제할 수 있도록 고의로 제작된 명령어들의 집합을 말한다.[65]

64) U.S. Department of Justice, Law Enforcement Administration, Computer Crime, Criminal Justice Resource Manual, 1982., p.25.등

65) Frederick B. Cohen, A Short Course on Computer Viruses, 2nd Ed, John Wiley and Sons, Inc., 1994, pp. 1-2., 163-164., Vesselin Bontchev, Methodology of Computer Anti-virus Research, Ph.D. Thesis, University of Hamburg, 1994, pp. 4-5.

나. 현황

1985년에 불가리아에서 제작된 브레인 바이러스(Brain Virus)를 시조로[66] 하는 컴퓨터 바이러스는 1987년까지 IBM 호환기종의 컴퓨터에 6개가 출현하는데 그쳤지만, 그 다음해에 매킨토시(Machintosh) 기종의 컴퓨터에 출현한 것을 비롯하여 1990년에 약 1,000개, 1993. 9.까지 3,000여개가 발견되었고,[67] 1995년에만 1,400여종이 새로이 출현함으로써 1996. 1.까지 세계적으로 약 7,400여종의 바이러스 프로그램이 제작되었다.[68]

국내에서도 1989년 3종의 바이러스가 제작된 것을 시작으로 1995년에 42종이 제작되기까지 모두 120여종의 바이러스가 만들어지고, 화일 바이러스(File Virus) 131종, 부트 바이러스(Boot Virus) 46종, 화일 부트 바이러스(File Boot Virus) 8종 등 모두 185종의 바이러스 프로그램이 발견되어[69] BBS와 불법복제를 즐기는 학생들에 의하여 교육기관의 컴퓨터들을 중심으로 배포되었다.[70]

다. 사례

1988년 서울 올림픽이 진행될 무렵, Internet에는 UNIX를 탑재한 모든 컴퓨터에 감염되는 24줄, 634바이트의 Bourn-Shell로 만들어진 Shell Program인 AT&T 바이러스가 발견되었는데 동 프로그램은 UNIX기종이나 Version을 가리지 않고 감염되어 컴퓨터 통신망에 엄청난 위기감을 조성하였다.

1995. 11. 바이러스의 존재를 은폐하는 암호화 프로그램인 스메그(Smeg)로 Pathogen과 Queeg라는 복잡한 은폐형 바이러스(Stealth Virus)[71]를 제작, 반포함으로써 세계 최초로 컴퓨터 바이러스와 관련하여 기소되었던 크리스토퍼 필(Christopher Pile)은 징역 1년 6월의 실형을 선고받았다.

1995. 말 미국에서는 대학출판사들이 정보자유화의 미명아래 덴마크의 룬 스카다마(Rune Skardhamar)가 쓴 "바이러스 예방과 퇴치(Virus Detection and Elimination)"라는 바이러스 관련책자를 발간하였는데 그 내용중에는 유명한 바이러스 제작그룹인 팔콘 스킴(Phalcon/SKIM)이 발행하는 전자잡지 40헥스(HEX)에 게재된 바이러스의 소스 프로그램(Source Program)을 포함하고 있어 사용자들의 PC에 바이러스가 감염되는 등 엄청난 파문을 일으킨 일도 있다.

우리나라에서도 "Dark Avenger" 바이러스나 "Michelangero" 바이러스에 의하여 상당수의 PC 사용자들이 하드디스크를 날리고 분통을 터뜨리는 사례를 주변에서 자주 보았다.

라. 전망

어떤 전문가는 금세기말까지 약 1만개의 Dos Virus를 예상하고 있다. "도전과 응전"의 법칙에 따라 Virus 퇴치방법에 대한 연구도 상당히 진척되고, DOS나 Machintosh, Amiga 등 종전의 단일체제(Stand-Alone) 중심의 운영체

66) Frederick B. Cohen은 전게서 pp. 33-34.에서 자신이 1983. 11. NSA의 위탁을 받아 가동하던 UNIX에서 발견된 것이 최초의 과학적인 Computer Virus라고 하지만, 사회적으로 문제를 야기한 것은 아니다.

67) Winn Schwartau, 전게서, pp. 104-105.

68) 중앙일보 '96. 2.6.자 28면.

69) 중앙일보, '95. 12.28.자 29면.

70) 상세한 것은 졸저, 전게서, p.320 이하 참조.

71) 감염된 화일의 크기가 변경되지 않은 것 처럼 하거나, 감염된 부분을 해독하려할 경우, 감염되지 이전의 메모리 내용을 보여주게 하는등 다양한 방법으로 검색자가 바이러스를 발견하지 못하도록 은폐하는 방법을 가진 바이러스 프로그램.

제와 메모리 운영방식이 전혀 다른 UNIX, OS2, Window NT등 다중운영체제의 확산으로 PC의 환경은 더욱 탄탄해지고 있지만, 과연 인간이 만든 Computer Virus들로부터 우리의 컴퓨터가 안전을 보장받을 수 있을지는 아무도 알 수 없다.

최근 미국 르하이(Lehigh) 대학의 컴퓨터 바이러스 연구소[72]와 독일 함부르그 대학의 바이러스 연구소[73]가 분석한 결과를 보면, 컴퓨터 지하세계(Computer Underground)의 일부 프로그래머들이 제작하는 바이러스와 윈도우즈(Windows) 운영체제에서 활동할 수 있는 새로운 유형의 바이러스들이 만들어내는 역기능은 매우 위협적이다.

특히, 바이러스를 검색하는 프로그램(Anti-Virus Program)들이 디버깅 방식(Debugging)으로 바이러스 루틴(Vector)에 대한 검색을 시도할 경우, 디버깅 자체를 방해하거나 바이러스의 코드를 변경하여 검색을 피하려는 디버깅 차단기술(Anti-Debugging Tricks)[74]은 바이러스 감염운영체제의 확산, 감염대상의 확장, 암호화를 통한 고도의 은폐기술과 함께 정보전쟁의 중요한 무기로 등장할 것임이 분명하다.

윈도우즈 '95가 보급되어 이를 기반으로한 응용 프로그램(Utility)들이 일반화되면서 DOS를 기초로 한 바이러스의 활동은 대단히 위축되었지만, 바이러스 검색 프로그램이 실행화일만 검색하는 약점을 이용한 MS-Word 6.0의 매크로 화일(Macro-File)에 대한 워드 바이러스(Word Virus)는 윈도우즈, 매킨토시를 불문하고 감염되어 한동안 기승을 부렸고, 최근에 윈도우즈 '95에 대한 본격적인 바이러스로 알려진 보자 바이러스(Boza Virus)는 다행스럽게도 한글 윈도우즈에는 작동할 수 없는 것으로 보고되었으나 일단 DOS와 메모리 운용방식이 다른 윈도우즈 '95에 대하여 본격적으로 바이러스가 활동할 수 있는 기법이 발견된 이상 바이러스의 활동은 중단되지 않을 것으로 보인다.

다음호에 계속

□ 著者紹介

최 영 호

1981년 건국대학교 법학과 (법학사)
1983년 건국대학교 법과대학원 (법학석사)
1983년 ~ 1986년 부산지방검찰청 검사
1986년 ~ 1987년 마산지검밀양지청 검사
1987년 ~ 1990년 수원지방검찰청 검사
1990년 ~ 1992년 마산지검 검사
1992년 ~ 1994년 서울지방검찰청 검사
현재 법무부 법무연수원 부장검사

72) Virus-l@Lehigh.edu

73) FTP.Informatik.uni-hamburg.de

74) Debugger가 인터럽트(Interrupt)를 못하게 하거나, 설정된 시간을 지키게 하거나, 디버거를 속이거나 디버거가 실행을 멈추도록 하는 방법, TD386 모드를 정지시키거나 V8086 프로세서를 일시정지하게 하는 방법등 사전차단법과 바이러스 루틴의 코드를 스스로 변경하는데 암호화 기법을 사용하여 간접적 효과를 발생하게 하거나, 실제로 바이러스 루틴이 변경되도록 기교를 삽입하는 기법이 있다. 상세한 것은 졸저, 전게서, p. 341이하 참조.