데이터베이스와 해커 Ⅲ

(Database & Hacker)

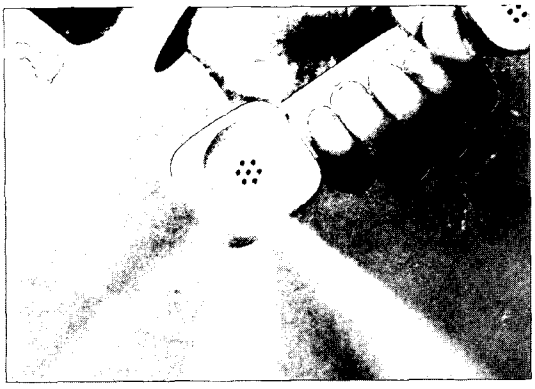
한상근
한국과학기술원 수학과 교수
Hahn, sang-geun. / Korea Advanced Institute of Science and Technology.

3. 해커의 현황 - 새로운 시대의 도래

공짜로 전화를 거는 기술도 역시 많은 해커들의 관심거리이다. 유명한 전화 해커라면 스튜 넬슨이나 존 드래퍼를 들 수 있는데, 존 드래퍼는 나중에 에스콰이어라는 월간지와의 인터뷰에서 공짜로 전화를 거는 비법을 독자들에게 공개해서 전화회사의 분노를 자아내기도 한다. 그 덕인지 존 드래퍼는 캡틴 크런치(아침식사용으로 우유를 부어서 먹는 바삭바삭한 일종의 칩같은 과자)라는 이름으로 잘 알려지게되고 이후에는 감옥에서 실형을 살기도 한다. 해커가 이렇게 실형을 사는 일은 참으로 드문데 실형을 사는 대개의 해커들

은 전화회사와의 문제가 원만하게 해결되지 않아서 감옥에 가는 경우가 제일 많다. 존 드래퍼는 FBI의 함정수사에 걸려서 다시한번 감옥에 가게된다. 일반 컴퓨터 회사와 달리 전화회사는 무료로 전화를 사용하는 이들을 지독하게 싫어한다. 이것은 아마도 해커의 실력이 모자라서 장거리 전화요금이 다른 사람에게 부과되고, 이 피해자가 전화회사에 찾아와서 잘못 부과된 고지서를 가지고 큰 소란을 일으키기 때문이다. 존 드래퍼가 캡틴 크런치라는 별명을 얻게된 것은 텔레비전에 캡틴 크런치 광고가 나오자 어느 친구가 휘파람을 불었는데, 존 드래퍼는 이 휘파람이 장거리 전화를 걸때에 들리는 주파수 2600 신호음과 같다는 사실을 알아낸 뒤부터이다. 스튜 넬슨이나 존 드래퍼가 시작한 가장 첫번째 일은 번호부에는 나와있지 않은 번호에 전화를 걸면 어떤 일이 생기는지를 알아내는 것이었다. 이 과정에서 전화국의 전용 번호를 알아내기도 하고 다른 지역국으로 접속하는 번호를 알아내기도 한다. 나중에는 프로그램을 만들어서 컴퓨터가 접속가능한 모든 전화번호를 모조리 걸어보도록 만든다. 전화선의 끝에 다른 컴퓨터가 있으면 그 컴퓨터는 해커의 컴퓨터에게 모뎀을 통해서 신호음을 보내고, 해커의 컴퓨터는 컴퓨터가 연결되어 있는 그런 전화 번호만을 기록해 놓는다. 이런 방식으로 자기 주변의 네트웍의 지도를 만들어가는 것이다. 영화 "워 게임"에도 주인공인 어린 학생이 이런 프로그램을 만들어서 사용하는 이야기가 있는데 이것은 벌써 수십년된 기법이다. 십년쯤 전에는 어느 고등학생이 캘리포니아의 전화회사 전산실 쓰레기통을 날마다 뒤져서 시스템을 이해하고 운영자의 비밀 번호를 알아낸 뒤에는 근처의 창고를 빌려서 전화기 부품회사를 만든 일이 있다. 파시픽 벨 전화 회사처럼 거대한 회사에서는 기본적으로 일 퍼센트 정도의 부품은 운송도중에 망가지거나 잃어버릴 가능성이 있다고 보고 이것을 일일이 챙기지 않는데, 망실된다고 여기는 이 작은 퍼센트의 범위 안에서 불법을 저지른 것이다. 이 학생은 자기 창고로 부품을 보내도록 전화회사의 컴퓨터를 조작하기도 하고 이렇게 받은 부품을 다시 파시픽 벨 회사에 팔기도 한다. 결국에 이 학생은 잡혀서 감옥에 다녀오는데 나온 뒤에는 컴퓨터 보안회사를 차린다. 이 회사의 광고 문안은 지금도 유명한 "도둑만이 도둑을 잡을수 있습니다" 이다. 금융기관의 이자 계산프로그램을 조작해서 계산의 결과로 나오는 원 미만의 끝수를 모두 자신의 구좌로 보내는 살라미 방식의 한 변형이라고 볼수 있는데(살라미는 아주 얇게 썬 이태리식의 소세지이다.), 대개의 사람들은 자기 통장에 남아있는 돈이 193만 9,563.4원이거나 아니면 193만 9,563원이거나 별로 신경쓰지 않을 것이다. 하지만 이런 끝수도 자동으로 모으면 상당히 큰 액수가 되기 마련이다.

해커들이 여러가지 해보고 싶은 일이 많을수록 나름대로 많은 지식과 장비가 필요한데, 지식은 네트웍에서 쉽게 배운다쳐도 돈은 공부한다고 해서 쉽게 얻어지는 것이 아니다. 유럽에서는 특히 독일과 네덜란드의 법이 해커에 대해서 관대해서 이들 나라에는 많은 해커들이 있는데 이들도 역시 돈이 있어야 해보고 싶은 일을 해볼수 있다. 네덜란드에서는 해마다 세계 해커 대회도 열린다. 1985년에 옛소련의 KGB



요원들이 당시 서독의 해커들에게 접근해서 미국의 인터넷에 침입하여 기밀 정보를 가져오면 KGB는 해커들에게 마약과 돈을 제공하겠다고 약속했다. 이들 해커들은 서독의 공중전화를 통해서 미국의 로렌스 버클리 연구소를 거쳐서 미국의 여러 국립 연구소, NASA, 일본과 유럽들의 여러 컴퓨터 네트웍에 침입해서 많은 자료를 훔쳐다 소련에 넘겨주었다. 엄청난 비밀 문서들이 넘어갔다고 언론에 나온적이 있지만 사실 인터넷으로 접속할 수 있는 컴퓨터에 저장하는 자료는 비밀로 분류된 자료가 아니다.

비밀로 분류된 자료는 외부와 연결되지 않은 컴퓨터에만 저장할수 있다.

이들이 소련에 제공한 자료는 민감한 대외비(Unclassified but Sensitive) 자료들 정도이다. 문제는 중요한 자료가 나갔다는데 있는 것이 아니라 자료가 오랫동안 새나가고 있었는데도 이 사실을 알지 못했다는 데에 있다. 이 사건의 실마리는 버클리의 연구소에 근무하던 어느 컴퓨터 계정의 사용자가 자기 계정의 사용료에 75센트의 오차가 생겼음을 인식하고 이 오차를 끈질기게 추적한데서 나타났다. 이 75센트의 차이가 왜 생겼는지를 알기 위해서 연구원 클리포드 스톨은 다음번에 언제 들어올지 모르는 해커를 밤을 세우면서 기다리기도 하고 FBI는 그럴듯해 보이는 엉터리 군사자료를 NASA의 컴퓨터에 저장해놓기도 하였다. 결국에 이들 해커들은 서독의 헌법 수호국과 미국의 CIA에 의하여 1989년에 서독 현지의 한 공중 전화기 앞에서 해킹 도중에 붙잡히게 되는데 이들중 한 사람은 뒤에 의문의 자살을 하고 나머지 사람들은 해커의 세계에서 매장당한다. 75센트로부터 이 사건을 추적하는 이야기는 스톨이 "뻐꾸기 알"이라는 책으로 출간한바 있다.

이 로렌스 버클리 연구소의 컴퓨터 시스템은 그 보안이 허술하기로 지금도 정평이 나있는데 작년에는 누군가가 각종 포르노 사진을 GIF 화일로 만들어서 버클리 연구소의 컴퓨터에 잔뜩 저장해 놓기도 하였다. 조사가 계속되면서 이런 포르노 사진들은 컴퓨터에 몇년씩이나 저장되었다는 사실이 밝혀졌다. 이 컴퓨터 센터는 몇년간이나 포르노 사진의 데이터베이스 역할을 하고 있었던 것이다.

1989년에 그런 큰 사건이 있었음에도 포르노 사진은 아무런 문제가 없었던 것이다. 필자도 이런 소문을 듣고서 버클리 연구소에 접속해서 그런 사진을 몇개 본적이 있는데 인터넷에 돌아다니는 보통의 포르노보다 야한 사진은 찾아 볼수가 없었다. 소문은 별로 믿을것이 못된다.

1990년 5월 9일에 미국 연방 검찰총장은 태양마 작전(Operation Sun Devil)을 발표하였다. 그동안 연방 정부차원에서 조금씩 준비하

고 있던 해커말살 정책이 마침내 공식 출범을 한것이다. 이틀 전인 5월 7일에 미국의 여러 도시에서 150명의 비밀 경호대(Secret Service: 미국의 비밀 경호대는 한국의 청와대 경호실과는 달리 재무부 산하 기관으로서 대통령의 경호 뿐만 아니라 위조 지폐의 적발, 신용카드 범죄의 단속, 통신 범죄의 단속등 몇가지 임무를 추가로 맡고있다.) 수사관들과 경찰들이 27개의 수색 영장을 집행하였다. 작전을 벌인 도시는 시카고, 로스엔젤레스, 마이아미, 뉴욕, 피닉스, 샌디에고 등 13개가 넘는다. 이날의 검찰총장의 발표는 해커들을 가장 파렴치하고 비열한 범죄자들로 묘사하는데 조금의 손색도 없었다. 해커들의 범죄라고 규정한 발표문의 일부를 보면 신용카드를 훔치고, 이런 장물 카드를 사고 팔고, 장거리 전화 비밀 번호를 불법으로 사용하고 컴퓨터에 불법으로 접속했다.

미국에서는 전화로 물건을 주문하고(예를 들면 우체국의 사서함으로 물건을 보내도록) 신용카드번호를 말해주면 카드로 요금이 청구된다. 따라서 남의 신용카드번호만 알면 얼마든지 물건을 살수있다. 혹은 은행에서 보내는 카드를 동봉한 우편물을 남의집 우체통에서 몰래 빼내서 서명한 뒤에 마음대로 사용할 수도 있다. 아니면 카드가 없는 타인의 이름으로 카드를 은행에다 신청하기도 한다. 공중전화에서 장거리 전화를 하고 요금은 자기집으로 청구되도록 할 수도 있는데, 통화하고 싶은 전화번호를 누르고 송화기에서 동전을 얼마 넣으라는 말이 들릴때에 자기 집 전화번호와 네 자리로된 비밀번호를 누르면 전화요금은 자기 집으로 청구된다. 따라서 전화회사의 시스템을 해킹할 만큼의 실력이 없는 해커는 역시 남의 비밀번호만 알면 공짜로 장거리 전화를 걸수 있다. 이런 자료시장은 미국내에서만 연간 몇십억불 규모라고 알려져 있다.

이 태양마 작전에는 AT&T, MCI, US Sprint 등 미국의 여러 장거리 전화회사와 다른 피해회사들이 참여했다. 1984년에 제정된 범죄 소탕법(Comprehensive Crim Control Act)에 근거를 두고 이년간의 계획 끝에 집행된 이 작전은 그 주된 목적이 이들 범죄자들(해커들)이 사설 비비에스(Bulletin Board Service)를 통해서 정보를 교환하고 배우는 것을 막기위함이라고 비밀 경호대의 차장은 기자 회견에서 발표했다. 이 작정의 목표가된 사설 비비에스의 대표적인 것은 아리조나주 피닉스시의 억만장자 아이들 비비에스(Billionaire Boys Cub computer bulletin board), 샌프란시스코의 평화네트(PeaceNet), 버클리의 우물(The Well) 이었다.

또한 단 한명도 구속하지는 않았지만 전국적으로 40대의 컴퓨터와 23,000장의 디스켓을 압수했다. 그리고 앞으로도 지속적으로 이 작전을 계속할 것임을 밝혔다. 비밀 경호대가 관할권을 가지는 장거리 전화나 신용카드등의 컴퓨터 관련 범죄의 용의자는 미화 1,000불 이상의 피해를 끼치면 10년 까지 징역형을 살수도 있다. 구속자가 단 한사람도 없는 이유는 집안에서 누가 컴퓨터를 사용하는지를 알수가 없기 때문이다. 이 과정에서 뉴욕의 어느 17세된 소년은 전화회사 몰래 불법 음성사서함 서비스를 설치하려다 붙잡히기도 했다.

이 태양마 작전이 비밀리에 진행되고 있던 도

중에 책임감있는 컴퓨터 전문가들(CPSR: Computer Professionals for Social Responsibility)은 하원 법사위원회를 통해서 컴퓨터 관련 범죄의 수사시에 피의자의 인권과 관계있는 몇개 질문을 한다. 1989년 8월에 정보 자유법에 근거해서 제출한 이 편지에 대해서 비밀 경호대는 컴퓨터진단센터(Computer Diagnostic Center)라고 부르는 화일자동검색프로그램이 있음을 인정했다. 이 검색 프로그램은 수많은 화일을 자동으로 검색해서 수사할 가치가 있어 보이는 화일들 만을 골라낸다.

지금은 인공 지능 기법을 사용하리라고 생각하는데, 전화통화에서도 키 워드 (예를 들면 특정인의 이름, 특정한 단어나 특정인의 목소리)를 찾아내는 프로그램이 있다. 이런 프로그램이 근본적으로 문제가 되는 것은 모든 사람을 아무런 정당한 이유없이 컴퓨터가 자동으로 감시하기 때문이다.

전화회사에 114 안내를 걸어본 사람은 느낄지 모르지만 모든 안내원들의 평균 작업시간이 컴퓨터로 기록된다. 그래서 매달 회사의 게시판에는 "이번 달의 전화번호 안내에 걸린 평균 시간은 안내 한건에 17.9초이고 일등을 한 사람은 우 ○○씨입니다. 우 ○○씨의 기록은 안내 한건에 평균 14.3초가 걸렸습니다."라는 등의 공고가 나붙게 된다. 물론 속도가 빠른 사람에게는 무엇인가 상이 주어지고 속도가 느린 사람에게는 무엇인가 좋지 않은 일이 생기기 마련이다. 이러니 안내원에게 "예? 몇번이라고요?" 라고 하면 신경질을 내는 것이다.

핸드폰이나 삐삐를 사용해도 사용자의 위치가 어느 지역인지 나오게 된다. 자동차에 조그만 발신기를 부착하도록 해서 고속도로 통행료나 도심 통행료를 받자는 계획이 건설교통부와 서울시에 있는데, 앞으로 운동권 학생들이나 노동운동하는 조합원들, 사업가 그리고 정치인들은 중요한 일이 있을 때에는 택시를 타고 다녀야 할일이다. FBI는 민간인들의 거듭된 요구에도 불구하고 정보자유법을 위반해가면서까지 그들이 사설 비비에스를 어떻게 얼마나 감시하는지에 대한 답변을 회피한다. 이 태양마 작전의 충격속에서 정보시대에 개개인 인간의 존엄성을 지키려는 움직임이 태동하고 이어서 전자전선재단(EFF: Electronic Frontier Foundation)이 태어난다.

이 재단에는 초기의 해커이고 애플 컴퓨터의 창업주의 하나인 스티브 워즈니악이 참가했다.

컴퓨터는 인간에게 봉사하고, 인간이 컴퓨터의 주인이되는 컴퓨터 시대를 꿈꾸던 해커의 이상은 아직도 남아있었고 이 태양마 작전은 인권 운동 단체들과 해커들을 한데로 묶어주었다.

재단이 제기한 문제들은 급변하는 정보사회에서 아직도 해결되지 않은 근본적인 법적, 사회적 물음을 포함하고 있다. 대개의 내용들은 지금의 법정에서 아직까지 한번도 다루어지지 않은 문제들이고 그런 문제를 의식하고 있는 사람의 수는 참으로 소수에 불과하다. 그 문제점들은 예를들면 "무엇이 언론의 자유이고, 무엇이 데이터인가? 그 둘의 차이는 무엇인가? 인터넷에서 장소나 주소란 무엇을 의미하는가? 어떤 제 삼자가 당신의 재산운영 상황을 자신이 소유하는 데이터라고 주장할수 있는가? 제 삼자가 당신의 버릇, 물건을 사는 습관이나 사

생활에 대한 기록을 자신이 소유하고 자신이 사고 팔수있는 상품이라고 주장할수 있는가? 어떤 사람이 자기는 ○○○○○에 관한 지식 그 자체를 소유하고 있다고 주장할수 있는가?"이다. 이런 상황을 더욱 어렵게 만드는 것은 수사기관이나 정부기관에서는 정보대기업의 이익을 위해서 일반인들이 무관심한 속에서 정보 대기업에 유리하도록 법과 관례를 만들어가고 있다는 점이다.

재단의 첫번째 사업은 책임감있는 컴퓨터 전문가들(CPSR)에게 27만 5천불을 지원해서 정보시대에 인권을 보호하는 일을 맡아달라는 것이었다.

책임감있는 컴퓨터 전문가들(CPSR)이 그들의 사업을 시작한 이유는 다음과 같다. 레이건 대통령이 1985년에 비밀 분류에 관한 새로운 대통령명령을 발동해서 정부기관의 자료에 민간인들이 접근하지 못하도록 하고, FBI는 전 미국의 모든 사람의 행적을 추적해주는 프로그램을 만들려고 한적이 있다.

이에 대한 반발로 책임감있는 컴퓨터 전문가들(CPSR)이 태어난 것이다. 모든 인간의 모든 감정과 행동이 숫자로 처리되는 공포의 미래 전체주의 사회로부터 인간의 존엄성을 지키려는 마지막 전선인 전자전선재단의 최전선은 이미 10년전부터 존재하고 있었다.

이 태양마 작전의 덕택으로 많은 사설 비비에스는 지하로 숨어들어갔다.

그러나 작년 12월 크리스마스에 컴퓨터 보안 전문가의 계정을 하이재킹해서 연구중인 자료까지도 훔쳐간 것을 보면 해커들 역시 이제는 본격적인 연구 집단이 생긴 모양이다. (하이재킹이란 계정의 주인이 컴퓨터를 사용하는 도중에 해커가 침투해서 그 계정을 이용하는 것을 말한다.

물론 그 계정의 주인은 해커가 일하는 도중에는 아무런 작업도 할수없고 해커의 작업을 화면을 통해서 보고만 있거나 아니면 전산소에 연락하는 수밖에 없다.

해커는 인터넷의 통신 프로토콜로 많이 쓰이는 TCP/IP의 약점을 이용해서 샌디에고 슈퍼컴퓨터에 침입했다. 접속시도를 할때에 컴퓨터끼리 어떤 숫자를 가지고 서로 확인하는 과정에 이 약점이 있다.

TCP/IP의 이론상의 이런 약점은 약 10년전에 AT&T의 연구원이 밝혀냈는데, 이 해커는 그 논문을 연구한 것으로 보인다.) 하이재킹을 당한 사람이 저명한 컴퓨터 보안전문가인 점에 충격을 받은 CERT (Co-mputer Emergency Response Team)은 곧바로 이에 대한 대책을 발표했는데, 몇몇 기종은 이에대한 방비책이 아예없다. 더 자세한 내용은 자신의 기종에 대해서 CERT가 뭐라고 했는지 찾아보아야 한다.

그리고 1990년대인 지금은 (아직까지는) 안전한 공개열쇠 암호의 발견으로 사회를 근본적으로 바꿀수 있는 여러가지 구상들이 정부 기관이나 해커들을 통해서 나오고 있다. 정부 기관등에서 구상하고 있는 기법은 민간인의 암호 사용금지(도청 하기 쉽도록), 주민등록증을 스마트카드로 바꾸기, 지폐를 스마트카드로 바꾸고 화폐를 없애기등이다. 이런 것들도 잠깐만 생각해보면 적용하기에 따라서 전 세계 단일 국가나 아니면 무정부 세계를 만들어낼 가능성이 있다. DPC