

해 / 키 / 비 / 상

당신의 데이터베이스는 안전한가?

Alarm! Hackers in Your Database!

임 태섭/ 광운대학교 신문방송학과 교수

Lim, Tae-seop./Kwang-Woon University

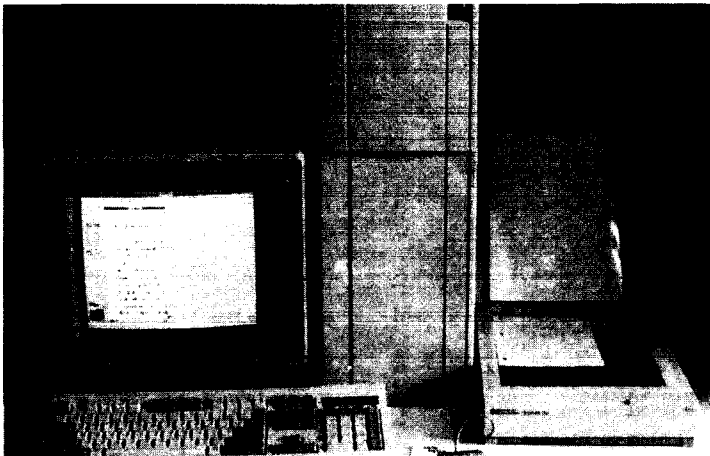
Department Journalism and Communication Studies

옛날 어느 부자(父子)가 같이 짚신장수를 했는데, 아버지가 만든 짚신은 날개 돋힌듯 팔렸지만 아들이 만든 것은 영 팔리지 않았다 한다. 아들이 불 때는 자기가 만든 짚신이나 아버지가 만든 짚신이 별로 차이가 없는데 어째서 아버지가 만든 짚신이 유독 잘 팔리는지를 몰라 아버지께 그 이유를 물었다.

그러나 아버지는 미소

를 지으며 정성껏 만들라는 이야기만 할 뿐 그 비방을 가르쳐 주지 않았다 한다. 그러다가 세월이 흘러 노환으로 죽음을 앞두고 된 아버지는 임종하는 아들의 귀에 모기같은 목소리로 “짚신을 다

만들었다고 그냥 팔려 하지 말고 너털너털 붙어 있는 지푸라기 자락을 떼어낸 다음 팔아보라”라고 일러주면서 “이 비방은 아무에게도 가르쳐 주지 말라”고 당부하였다



한다. 물론 아버지의 비방을 따라 만든 아들의 죄
신은 다른 사람들이 만든 것보다 훨씬 잘 팔렸을
것이다.

이 설화는 자기만이 알고 있는 비방을 남에게
알려주고 싶어하지 않던 우리네 장인문화를 이야
기할 때 자주 등장하는 것이다. 아들이 어찌 남이
겠는가 마는 아들이 알게되면 아들의 처남이 알
게될 수도 있고 그러다 보면 모든 사돈댁 식구가
알게 되고, 사돈의 사돈이 알게되어 마침내는 모
든 짚신장수가 다 알게되는 것이 아니겠는가?

따라서 아들에게까지 비밀을 숨겼다 하여 비정
한 아버지라고 욕할 수는 없는 것이다.

사람은 누구나 자신의 비방을 혼자만이 간직하
고 싶어한다. 자신이 오랜 연구와 경험을 통하여
획득한 지식을 남에게, 특히 자신과 경쟁하는 입
장에 놓인 사람들에게 알려주고 싶어하는 사람이
어디 있겠는가?

현대인도 마찬가지이다. 자신만의 노력으로 일
구어 놓은 텃밭을 경쟁자에게 내어 줄 사람은 없
다. 그러나 현대인은 위 이야기에 나오는 짚신장
수 노인과 같은 행복한 입장에 놓여 있지 않다.
짚신장수 노인은 모든 노하우를 자신의 머리속에
저장해 두었기 때문에 자기가 발설 하지 않는 한
누구도 그 지식에 접근할 수가 없었다. 그러나, 현
대인의 지식은 복잡하여 더 이상 사람의 머리속
에 저장될 수 있는 성질의 것이 아니다. 따라서
현대인은 두뇌의 기억장치를 확장 할 수 있는 보
조기억장치를 개발하기 위하여 끊임없이 노력해
왔으며, 20세기 후반에 들어 급속도로 발전한 컴
퓨터는 데이터베이스의 형성을 가능케 함으로써
현대인의 고민을 해결해 주는 듯 하였다. 그러나,
컴퓨터를 통한 데이터베이스가 인간의 두뇌와는
비교할 수 없는 막대한 저장능력을 가지고 있음

에도 불구하고 인간의 두뇌가 가지고 있는 기밀
유지기능을 따르지 못하기 때문에 에 평생을 바쳐
이룩한 연구가 하루 아침에 다른 사람의 손에 넘
어가는 일이 생겨나고 있다.

최근 들어 우리는 연일 컴퓨터 해커에 대한 보
도에 접하고 있다. 한 영국인 소년이 우리 원자
력연구소 데이터베이스에 침투하여 중요한 기술
정보를 빼내어 갔다는 보도의 충격이 채 가시기도
전에 어느 한국인 해커가 벨기에의 유럽암연
구센터에 침투해 기밀자료를 빼내었다는 보도에
접해 야 했다. 인터폴까지 나선 수사결과 그 해커
는 한국인이 아니라 스위스인이라는 것이 밝혀졌
지만 더욱 충격적인 것은 그 스위스인 해커가 한
국의 컴퓨터를 경유하여 마치 한국인이 침투한
것처럼 가장할 수 있었다는 점이다.

충격은 여기서 끝나지 않는다. 영국인 소년의
원자력연구소 침투사건의 수사결과 이 해커가 원
자력연구소의 데이터베이스를 두차례 이상 침투
했음에도 불구하고 원자력연구소가 전혀 그 사실
을 모르고 있었다는 것은 또 하나의 충격을 안겨
주었다.

국제해커의 활약은 「인터넷」과 같은 국제통
신망의 확장 때문이라고 할 수 있다. 인터넷은
세계각처의 주요 컴퓨터 시스템을 상호 연결함으
로써 정보의 빠르고 폭넓은 교환을 가능케 하는
아주 유용한 시설임에 틀림이 없다. 그러나 이러
한 시설은 원거리 해킹을 가능케 함으로써 정보
의 기밀유지를 더욱 어렵게 하고 있다. 그러나, 컴
퓨터의 정보누출은 유선통신망을 통해서만 이 루
어지고 있는 것은 아니다.

최근의 보도에 의하면, 컴퓨터의 키보드 등에서
나오는 전파를 증폭 시켜 컴퓨터에 입력되고 있
는 내용을 알아내는 「PC도청」까지 생겨나고 있다

고 한다. 이제 우리의 기밀정보는 유무선을 통한 갖가지 침투행위에 거의 무방비한 상태로 노출되어 있는 것이다.

현재 데이터베이스 소유자가 가진 유일한 방비책은 암호이다. 대부분의 암호는 숫자와 영어 알파벳의 조합으로 이루어져 있어서 그것을 모르는 사람이 정확한 암호를 찾을 확률은 수백만분의 일도 되지 않는다.

그러나 이것은 산술적 확률일 뿐이다. 암호란 그것을 만든 사람이 기억하기 좋게 만들어지는 수밖에 없기 때문에 그 사람의 주변정보만 확보하고 있으면 암호를 찾을 확률은 의외로 높은 것이다. 그리고 암호에 대한 한 가지 불변의 원칙이 있다. 모든 암호는 풀리기 위해서 존재한다는 것이다.

아무리 어려운 암호일지라도 가용한 정보를 총동원하여 경우의 수를 좁혀 놓고 오랫동안 이리저리 맞추다 보면 결국에는 풀리고 마는 것이다. 해커라는 용어도 특별한 기술 없이 단순하고 반복적으로 이리저리 찢어보는 사람을 빗대어서 생겨난 것이다.

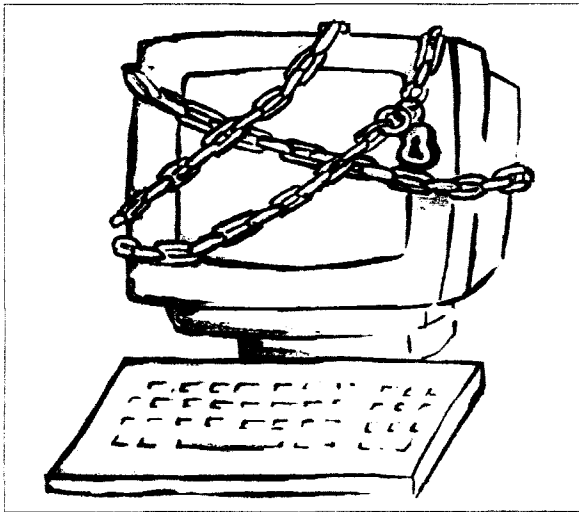
암호가 효과적인 방비책이 아니라면 우리는 어떤 다른 대책을 갖고 있는가? 그 답은 우리가 일반적인 「도둑질」을 예방하는 방법에서 찾아야 한다. 도둑을 막기 위해서 담장을 높게 쌓을 수도 있고 금고를 단단하게 해 볼 수도 있고 열쇠를

복잡하게 만들 수도 있다.

그러나, 이것은 데이터베이스의 암호와 같은 것이다. 뛰어난 도둑에게는 무용지물이다. 도둑이 없는 사회가 되기 위해서는 세가지 조건이 동시에 만족되어야 한다.

첫째는 사람들이 높은 윤리의식을 가져야 한다. 남의 재산을 탐내는 것이 얼마나 나쁜 것인지 그리고 왜 나쁜지를 알고 있어야 한다는 것이다.

둘째는 도둑질에 대해서는 엄한 처벌이 뒤따라야 한다는 것이다. 법으로 뒷받침되지 않는 윤리의식은 약해지기 마련이다. 남의 것을 훔치다가는 자신의 인생이 끝장나고 있다는 사실을 알 때 윤리의식은 더 끈고



해지는 것이다.

셋째는 도둑에 대비한 엄중한 경계가 있어야 한다는 것이다. 담장과 자물쇠만 믿고 집을 비울 것이 아니라 언제나 집안경계를 튼튼히 함으로써 도둑이 뚫고 들어올 틈을 줄여야 한다는 것이다. 이 세 조건 중에서 처음 것은 사회 구성원 모두에게 해 당되는 것이고 두번째 것은 정부가 나서서 할 일이며, 마지막 것은 집주인이 알아서 할 일이다.

데이터베이스로부터 기밀정보를 빼내는 것은 「정보 도둑질」이다.

이 정보 도둑질이 없는 사회가 되기 위해서 사

회 구성원들은 정보적 재산에 대한 윤리의식을 확고히 하여야 하며, 정부는 위반 행위에 대한 엄중한 처벌책을 마련해야 하고, 데이터베이스 관리자들은 그 데이터베이스에 출입하는 모든 사람들의 행위를 철저히 감시하여야 한다.

그러면 정보 도둑질을 예방하기 위한 이 세 가지 대책을 하나씩 살펴보기로 하자.

첫째, 무엇보다도 중요한 것은 모든 사용자가 남의 정보적 재산을 존중하는 마음을 가져야 한다. 정보를 훔친다는 것은 남의 돈을 훔치는 것과 조금도 다를 바가 없다.

열심히 일하여 벌어들인 돈을 훔친다는 것이 죄악이듯이 오랫동안 연구하여 축적해 둔 남의 연구결과를 몰래 빼내는 것 역시 흉악한 범죄이다. 남의 데이터베이스에 들어있는 정보를 빼내는 것을 단지 "기밀누출" 정도로 생각해서는 안된다.

기밀누출이란 비밀로 되어 있던 사항이 다른 사람들에게 알려지는 것에 불과하다.

따라서 기밀누출이 일어나는 경우에 한 연구자의 개인적 정보가 새어나가게 되어 그 연구자가 피해를 입게 되는 것은 사실이지만, 그 정보가 그 연구자의 업적이라는 사실은 인정되기 때문에 일생의 연구업적이 물거품으로 변하지는 않는다.

그러나, 정보 도둑질은 비밀누출에 끝나는 것이 아니라 그 연구결과에 대한 연구자의 공적마저도 가로채는 결과를 낳는다. 정보를 훔친 자는 훔쳤다는 사실을 감추기 위해서 그 연구결과가 마치 자기의 업적인 것처럼 가장하게 되고, 따라서 원래의 연구자는 연구결과가 가져다 줄 재산상의 이익을 잃게되는 것은 물론 그 연구결과에 대한 자신의 공적마저도 주장할 수 없게 된다. 결국 정보 도둑질이란 기밀과 공적을 동시에 훔치는 이중적인 도적행위인 것이다.

기밀을 훔치는 것만이 도둑질이 아니고 공적을 훔치는 것 역시 도둑질이라는 사실은 공공 데이터베이스 이용에 있어서도 정보 도둑질이 생겨날 수 있다는 것을 의미한다.

공공 데이터베이스에 저장된 정보는 누구나 이용할 수 있는 것이기 때문에 이미 기밀은 아니다. 따라서 누구나 마음 대로 이 정보를 사용해도 좋다고 생각하기 쉽다.

그러나, 실상은 그렇지 않다. 누구나 사용할 수 있는 것은 사실이지만 마음대로 사용할 수 있는 것은 아니다. 마음대로 사용할 수 없다는 말은 공공 데이터베이스로부터 얻은 정보를 마치 자기가 개발한 정보처럼 "써먹어서는" 안된다는 것이다. 공공 데이터베이스로부터 얻은 정보를 자기것인양 공표한다든지 남에게 멋대로 팔아넘긴 다든지 하는 행위는 남의 공적을 가로채는 흉악한 도둑질이다.

따라서, 아무리 공개된 정보일지라도 남이 연구한 결과라면 그것을 공표할 때 반드시 그 원저자를 밝혀서 그 공적을 인정해야 하며, 이 정보를 이용해 사업을 하는 경우에는 사전에 그 원저자의 동의를 얻어야 한다.

둘째, 정보 도둑질을 예방하기 위해서 정부가 할 일은 정보 도둑질에 대한 엄중한 처벌책을 마련하고 이를 적극적으로 시행하는 것이다. 오늘날의 사회는 일반적으로 블루칼라 범죄보다는 화이트칼라 범죄에 더 관대한 경향이 있다. 블루칼라 범죄란 절도와 살인을 위시한 물리적인 범죄를 일컫는 것이며, 화이트칼라 범죄란 뇌물, 횡령, 경제범죄 등 비폭력적 범죄를 일컫는 것이다.

정보 도둑질도 화이트칼라 범죄 중의 하나이기 때문에 사회치안에 직접적인 영향을 미치지 않아 관계기관들은 이를 예방하기 위한 적극적인 노력

을 보이고 있지 않다.

최근, 우리 정부는 형법에 「컴퓨터 해커」행위에 대한 처벌규정을 신설하여 국회의 심의에 회부하였다 한다. 이 시안에 따르면 컴퓨터 해킹은 10년 이하의 징역 또는 500만원 이하의 벌금형에 처할 수 있다고 한다. 사실 컴퓨터 해킹이 갖는 죄질의 흉악성에 비추어 볼 때 이 처벌규정은 매우 관대한 것이다. 컴퓨터 해킹이 한 사람 또는 한 기관을 파멸에 이르게 할 수 있다는 가능성을 생각해 본다면 그 형량은 이보다 훨씬 높아야 할 것이다.

형량의 경중보다 더 중요한 것은 관계기관이 어느 정도 성의를 가지고 컴퓨터 해킹을 수사할 것인가 하는 것이다. 피해자가 범인을 찾아 고발할 경우나 인터폴이 범인을 잡아 올 경우에만 이 법을 적용해서 처벌할 것이라면 이 법의 실효성은 거의 없는 것이다.

정부는 컴퓨터 해킹을 단순한 범죄로 보고한 두 조항으로 그 처벌을 규정한 후 잡히면 벌하겠다는 소극적인 자세를 버려야 한다. 컴퓨터 해킹의 다양한 유형과 그로 인한 피해의 종류를 잘 파악하여 컴퓨터 해킹의 처벌규정을 보다 세분화할 필요가 있으며 해킹에 대한 단속방안도 함께 마련하여야 할 것이다.

마지막으로 데이터베이스 관리자들은 그들 나름대로 할 일이 있다.

도둑의 비도덕성이나 정부의 무성의만 한탄하고 있을 것이 아니라, 스스로 자신의 재산을 지킬 수 있는 방법을 강구하여야 한다. 전술한 바와 같이 암호는 더 이상 만능수문장이 아니다.

아무리 좋은 자물쇠를 걸어두어도 문은 언젠가는 열리기 마련인 것이다.

가장 좋은 방법은 실내에 감시시설을 설치하여 문을 열고 들어오는 사람들이 무슨 짓을 하는가를 지켜보는 것이다.

보안이 잘 되어있는 기관의 감시체계를 보면 건물내 요소요소마다 감시 카메라를 설치해 놓고 감시요원은 중앙통제실의 모니터 앞에 앉아 건물안에 들어온 사람들이 무슨 짓을 하는지를 주시하고 있다.

컴퓨터의 데이터베이스 시스템도 이런 감시체계를 확보해야 한다.

현재 몇명의 사용자가 데이터베이스에 접속되어 있으며, 그들의 호스트 컴퓨터는 어떤 컴퓨터이며, 그들이 접근하려고 하는 정보는 어떤 정보이며, 그 정보에 접근하는 방법이 얼마나 정상적인지를 점검하는 기술적 방법을 고안하여야 한다.

그리고 어떤 사용자가 기밀정보에 접근하고 있을 때는 역으로 그 사용자를 추적함으로써 그가 정당한 사용자인지 아닌지를 확인할 수 있어야 한다. 컴퓨터 해킹은 데이터베이스와 컴퓨터 통신망의 발전으로 인하여 생겨난 새로운 유형의 사회적 범죄이다.

이는 건전한 연구분위기와 개발의욕을 저해함으로써 사회의 발전에 커다란 해를 끼치는 흉악한 범죄행위이다. 이를 방지하기 위해서는 데이터베이스 사용자와 정부 그리고 데이터베이스 관리자들이 삼위일체가 되어 최선의 노력을 경주하여야 할 것이다. **DB**