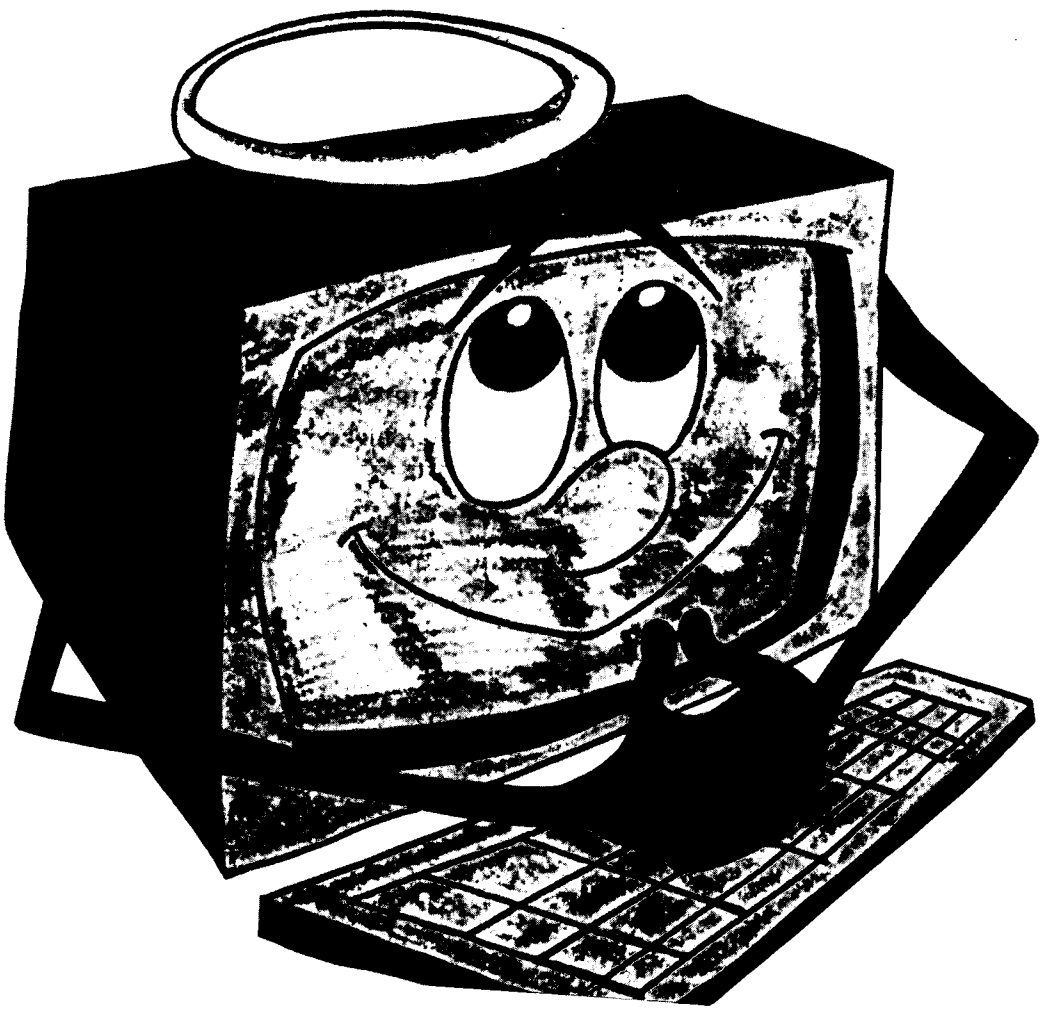
잠깐만

통신에서의 해킹 행위



천리안에서 "청와대"의 통신 ID를 도용하여 자료를 얻은후에 금융망에 침입하려 했다는 해커가 검거된 TV보도가 있었다. 이정도면 해커가 아니라 간커(?)라고 해도 과언이 아닐 지경이다. 컴퓨터 통신이 급격히 확산되면서 통신서비스 회사의 중앙시스템에 몰래 침입

하거나 다른 사용번호 (ID)를 훔쳐서 다른 목적에 이용하려는 해커들의 움직임이 심심찮게 보이는 것 같다. 통신망 침투는 아주 간단한 방법부터 고도의 컴퓨터 운영 지식이 요구되는 테크닉까지 동원되기도 한다. 실제 이러한 예는 역사가 4-5년 밖에 안되는국내 컴퓨터 통신에서 끊이지 않고 일어나고 있다. 몇년동안 하이텔이나 천리안에서 발생된 해커 침투의 사례를 보면 기발한 방법부터 어처구니 없는 방법까지 별별 수법이 총동원된다. 그중 중앙 시스템에 침투하는 사례는 그 해커의 침투행위가 확연하게 드러나거나 서비스 회사가 해커 침입경위를 밝히기 전까지는 드러나지 않아 별로 알려진것이 없다.

국내 컴퓨터 통신발전과 역사를 같이한 관계자의 말에 따르면 예전에 해커가 침입해서 접속시에 나타나는 로고를 거의 알아볼듯 말듯하게 수정을 해놓아 자신이 침투했었음을 경고한 적이 있다고 하여 해커들의 극성은 이제 우리에게도 심각한 문제가 되었음을 일깨워 주었다. 컴퓨터 통신의 도용 사례중 가장 많이 일어나는 것은 타인의 ID를 도용하는 예이다. 수법도 다양하여 "새로운접속 전화번호" 라고 해서 엉터리 전화번호부 형태로 공개자료실에 올려놓으면 그것을 받아간 사람들이 접속했을때 천리안이나 하이텔과 똑같이 생긴 초기화면이 나타나 ID와 비밀번호만 넣으면 중간에서 가로채서 도용하는 방법, 모뎀의 기계적 불량여부와 잡음을 테스트하는 프로그램이라면서 테스트를 위해 접속하면 비밀번호를 미리 정해진 해커의 ID 앞으로 메일로 보내는 방법, 접속을 편리하게 하기위해 ID와 비밀번호를 넣어 놓은 스크립트 화일(자동접속)을 같은 스크립트를 이용해서 메일전송으로 탈취해가는 방법, 가장 많이 쓰이는 통신에뮬레이터를 몰래 변조시키거나 비슷한 기능의 프로그램을 만든후 일정한 상황 변수가 맞으면 비밀번호를 탈취하는 방법 등 여러가지 방법으로 통신의 비밀번호를 도적질해간다.

대개 이러한 수법들은 외국의 유명 해커들이 썼던 방법을 책이나 지하 BBS 등을 통해서 얻는 경우가 많다. 특히 통신망에 직접 침투하는 경우는 많은 해커들의 목표가 되고 있으나 대형 컴퓨터 운영프로그램에 대한 고도의 지식이 요구되므로 해커의 침투 사례는 생각보다 그리 많지는 않다. 그러나 만약 실제 침투하여 시스템의 작동을 훼손했다고 해도 위신 실추를 우려한 회사측에서는 그대로 발표하는 경우가 드물어서 드러나지 않게 된다.이런 통신망 침투나 ID 도용 사례의 피해는 직접적으로 나타난다. 통신망에 침투해서 시스템 운영을 엉망으로 만들어 버리면 서비스 중지때문에 피해를 보게되며 ID를 도용당했을 경우 저질행위나 사기행위에 대해서 그 당사자가 책임을 져야 하기 때문이다. 특히 ID 도용의 경우 정액제인 하이텔에서는 별문제가 없으나 쓰는 만큼 추가되는 종량제인 천리안에서는 거의 치명적이다. 실제 한달전 필자가 알고 있는 의료인 한분이 ID를 도용당해서 수십만원에 이르는 사용료를 물어야 했다. 해킹 행위는 일부에게 컴퓨터 실력을 과시하는 영웅으로 떠받들여질지 모르나 컴퓨터 바이러스 같이 참으로 피곤한 것이다. 종량제인 경우에는 피해가 막대하기도 하며 도용된 ID라는 익명으로 포장된 저질게시물로 통신의 질적하락을 만드는 계기이기도 하다. ID 도용은 비밀번호만 관리를 잘하면 거의 예방할수 있는 것이므로 좀더 주의만 기울인다면 못된 해커들로 도용행위 결과로 인한 "억울한 통신인" 되는 경우가 없을 것이다. DB