백도어 없는 세상을 희망하며

김민찬

나는 이 에세이를 통해 정부가 범죄 예방 및 수사를 목적으로 요구하는 백도어가 본래의 취지를 벗어나 악용될 가능성이 높으며, 해킹 등을 통해 다른 집단의 손에 넘어가면 더욱 심각한 보안 위협이 될 수 있음을 주장한다. 영국 정부가 Apple에 iCloud 백도어 제공을 요구한 사례와, 미국 국가안보국(NSA)이 발견한 SMB 규약(Protocol)의 취약점이 악성코드 유포에 악용된 사례를 중심으로, 백도어의 존재 자체가 개인 정보 보호에 큰 위협이 될 수 있음을 주장한다. 또한, 이러한 백도어는 개인의 개인 정보 보호 노력을 물거품으로 만들 수 있음을 강조하며, 백도어 없는 안전한 디지털 환경을 위한 사회적 관심의 필요성을 주장한다.

현대 사회에서 나와 같은 컴퓨터 과학 전공자에게 있어서 가장 큰 보안 위협은 내가 이용하는 웹사이트가 해킹당해 개인 정보 또는 민감한 정보가 유출되는 것이라고 생각한다. 나는 전송 계층 보안(Transport Layer Security, TLS)이 적용되지 않은 웹사이트에는 중요한 정보를 입력하지 않으며, 공공 와이파이 대신 셀룰러 네트워크(Cellular Network)를 사용하고, 의심스러운 파일은 다운로드하지 않는다. 이 외에도 보안을 위한 다양한 수칙들을 지키며 살아가고 있다. 이러한 습관은 정확히 나를 목표로 한 공격이 아닌, 일반적인 피싱 공격이나 중간자 공격 같은 '아무나 걸려라'식의 무차별적인 공격에 대한 저항성을 높여준다고 믿는다. 그리고 현실적으로 내가 엄청난 부자가 된다거나 테러와 같은 중대한 범죄를 저지른다거나 하지 않는 이상, 정확히 나를 대상으로 한 공격이 일어날 가능성도 매우 낮으므로, 나의 잘못된 행동으로 인해 개인 정보가 유출될 일은 사실상 없다고 생각한다. 하지만, 내가 신뢰하는 웹사이트 - 이를테면 네이버나 구글과 같은 거대 플랫폼 - 가 공격당한다면 이야기가 달라진다. 이러한 경우 내가 손 쓸 수 있는 일은 거의 없다. 다른 웹사이트의 비밀번호를 바꾸거나, 신용카드를 정지시키는 등 개인 정보 유출로 인해 발생할 수 있는 이차적인 피해에 대비하는 방법만 남게 된다.

워싱턴 포스트(The Washington Post)에 의하면, 최근 영국 정부가 미국의 전자기기 제조 업체 Apple에게 클라우드 서비스 iCloud에 암호화되어 저장된 사용자 정보를 복호화하여 열람할 수 있는 백도어(Backdoor)를 제공할 것을 요구했다고 한다. 영국 내 iCloud 사용자뿐만이 아니라, 전 세계 iCloud 사용자를 대상으로 한 백도어를 요구했다는 특이 사항이 존재한다. 이 요구는 2016년 제정된 영국의 조사권 법(Investigatory Powers Act 2016)에 근거한 것으로, 해당 법은 영국의 정보기관과 법 집행 기관이 영장 없이 통신 내용을 감청할 수 있도록 허용하고, 영국의 통신 서비스 제공자(Communication Service Provider)에게 통신에 적용된 암호화의 해제를 요구할 수 있는 권한을 부여한다.

이 사례를 제시한 이유는 영국 정부가 요구한 백도어가 영국에 살지 않는 나의 개인 정보를 침해하는 용도로 사용될 수도 있기 때문이다. 이 사례를 바탕으로, 나는 이 에세이를 통해 어떠한 종류의 백도어든 - 심지어 범죄 예방 및 수사를 위한 선한 목적으로 생겨난 백도어라도 - 허용되어선 안 된다는 주장을 펼치고자 한다.

첫 번째 이유는 해당 백도어가 원래의 목적대로 쓰이지 않을 수 있기 때문이다. 백도어에 대해 많은 사람들이 가지고 있는 우려가 바로 이 부분이라고 생각한다. 영국 정부가 아무리 범죄 예방을 위해서 백도어를 사용한다고 이야기하더라도, 우리 같은 일반인들은 해당 목적으로 백도어가 선하게 사용되고 있는지 알 수 있는 방법이 없다. 그렇기 때문에 백도어가 잘못된 목적으로 사용되어도 정부 기관을 견제하기 쉽지 않다. 영국 정부가 아닌 중국 정부에게 백도어가 제공되었다고 생각해보자. 백도어가 인권 운동이나 민주화 운동을 탄압하는데 사용될 가능성이 매우 높다. 또한 범죄자를 대상으로 수사 목적으로 백도어가 사용된다고 하더라도, 범죄자의 데이터 중 범죄와는 관련이 없는 민감한 데이터 또한 백도어에 의해 함께 수집될 수 있다. 범죄자가 근무하던 기업의 기밀 정보, 가족이나 친구와 나눈 사적인 대화, 추억이 가득한 사진 등이 모두 법 집행 기관에 의해 수집되어 열람될 수 있다. 이는 개인 정보 보호에 대한 심각한 침해이다.

두 번째 이유는 해당 백도어가 다른 악의적인 집단에 의해서 사용될 가능성을 배재할 수 없기 때문이다. Apple이 결국 영국 정부에게 백도어를 열어줬다고 가정해 보자. 그런데 그 백도어가 영국 정부에 의해서만 사용될 것이라고 장담할 수 있을까? 오래된 사례이긴 하지만, 2017년에

워너크라이(WannaCry)라는 랜섬웨어(Ransomware)가 Windows 운영체제의 SMB 규약(Protocol)의 취약점을 이용해 유포된 사례가 있다. 이 취약점은 원래 미국 국가안보국(NSA)이 발견한 것이었고, 해커 그룹 Shadow Brokers에 의해 유출되어 결국 해당 랜섬웨어에 사용된 것이었다. 위 사례와 유사하게, 만약 영국 정부가 해킹당하여 해당 백도어가 외부로 유출된다면 선한 목적이 아닌 불순한 목적으로 백도어가 사용될 가능성이 높다. 백도어가 어떻게 구현되었는지 여부에 따라, 유출 후 백도어의 즉각적인 차단이 불가능할 수도 있다. 예를 들어 모든 데이터의 암호를 풀 수 있는 마스터키가 백도어로써 제공된다면, iCloud에 저장된 모든 데이터를 새로운 마스터키를 이용해 다시 암호화하기 전까지는 백도어의 완전한 차단이 불가능할 수 있다. 최근에 GS리테일이 해킹당해 158만 건의 개인 정보가 유출되었다. 의도적으로 만든 백도어가 없는데도 해킹으로 인해 개인 정보 유출이 다양한 곳에서 빈번하게 발생하고 있는데, 의도적으로 백도어를 만들어 둔다면 해킹의 위험성이 증가하게 됨은 자명하다.

Apple이 영국 정부의 백도어 요구에 굴복한다면, 나 역시 영국 정부에 의해 감시당할 위험에 처할 수 있다. 현재 Apple은 영국 정부의 요구에 대응하여, 영국 사용자에 한해 iCloud의 고급 데이터 보호(Advanced Data Protection) 기능을 비활성화했다. 이 기능은 iCloud에 업로드되는 데이터를 종단간 암호화(End-to-End Encryption)하여, Apple조차도 임의로 사용자 데이터를 복호화하는 것을 불가능하도록 만든다. 지금까지는 영국 밖 사용자에게는 직접적인 영향이 없지만, 영국 정부가 계속해서 앞서 언급한 것과 같은 종류의 더 강력한 백도어 제공을 요구하고 Apple이 이에 굴복한다면 이야기는 달라진다. 더욱이, 조사권 법은 통신 서비스 제공자가 영국 정부의 백도어 요구 사실을 공개하지 못하도록 제한한다. Apple 외의 다른 기업들은 이미 영국 정부의 요구에 조용히 굴복했을 수 있다. 나는 개인 정보 보호를 위해 개인으로써 할 수 있는 최선을 다하고 있지만, 지구 반대편 가본 적도 없는 나라에 의해 내 개인 정보에 대한 위협이 조금씩 커져가고 있다.

백도어 논란은 특정 국가만의 문제가 아니라 전 세계적으로 발생하고 있는 논란이다. 영국뿐만이 아니라, 우리의 우방국인 미국도 내가 사용하는 전자기기나 웹사이트 어딘가에 백도어를 숨겨놓았을 가능성이 높다. 미국이라면 심지어 백도어 없이도 암호화된 데이터를 수학적으로 해독할 수 있는 기술을 보유하고 있을지도 모른다. 물론 내가 이러한 공격의 직접적인 대상이 될 가능성은 낮다. 하지만 중요한 것은 개인 정보가 유출될 수 있는 경로가 존재한다는 것이며, 컴퓨터 과학 전공자이고 개인 정보 보호에 관심이 많은 나로서는 이를 무시하기 어렵다.

인터넷 시대에서 사생활 보호는 필수적인 권리이며, 이를 위해 개인 정보 보호에 대한 전 세계적인 관심이 필요하다. 우리는 기본적인 사생활을 보장받길 원하며, 헌법과 인권은 이를 권리로써 보장하고 있다. 우리의 삶이 점점 더 인터넷에 의존하게 되면서, 우리의 사생활의 영역은 클라우드와 인터넷 서비스로 확장되었으며, 당연히도 이 공간에서의 사생활 역시 보호받아야 마땅하다. 개인 정보 유출과 감시의 걱정 없이 인터넷을 자유롭게 사용할 수 있는 미래를 만들기 위해 사생활 보호에 대한 전 세계적인 관심이 필요하다. 치안을 이유로 사생활을 일부 포기하는 것이 아니라, 오히려 정부 기관에 의한 사생활 침해 시도를 막기 위해 우리의 권리를 주장해야 한다.

> "테러범을 뺀 나머지에게만 안전한 메신저 기술이란 없습니다. 안전한가 아닌가 둘 중 하나입니다."

Telegram 개발자인 파벨 두로프가 한 말을 인용하며 글을 마무리한다.