Korean banking system은 PKI(digital certificates)를 기반으로 만들어졌다. private key가 노출되면, 누군가 자신을 사칭하여 온라인 transactions을 수행할 수 있으므로, private key의 보호가 PKI에서 가장 중요한 부분이다.

Korean banking system은 passwords로 암호화된 private keys 파일을 user의 hard disk에 저장한다. 여기서 2가지 문제점이 있다. 1. privilege-escalation attack이 성공하면 memory에서 해독된 key를 읽을 수 있다. 2. 보안이 암호에 passwords에 의존하며, brute-force attack이나 key logging을 사용하는 malware로 훔칠 수 있다.

Korean banking system은 인증을 위해서 passwords, OTP, digital certificates의 조합이 필요하지만, 가장 중요한 private key가 오직 passwords로만 보호되기 때문에 digital certificates가 불필요하다. 만약 private key를 확실하게 보호할 수 있다면, PKI만으로도 인증하는데 충분하다.

Korean banking system의 digital certificates 사용의 문제점을 해결하기 위해서는 private key를 보호하는 수단을 강화할 필요가 있다. 현재 user의 hard disk와 같은 storage나 외부 저장장치인 USB에 보안 인증 매체 파일들이 저장되어 사용되고 있다. 나는 이를 넘어 user가 지정한 devices에서만 banking system을 사용하도록 하면 보안이 더 강화될 수 있다고 생각한다.

private key를 암호화하는 과정에 passwords 뿐만이 아니라, banking system을 접속하는 device의 고유 번호와 같은 것을 추가로 사용하는 과정을 거치는 것이다. 처음에 banking system에 passwords와 사용할 device(PC, Smart phone)s 들을 등록하고, 이후에 banking system을 사용할 때마다 passwords와 접속하는 device를 통해 암호화된 key를 기존의 private key와 비교하는 과정을 거치면 위 문제점을 해결할 수 있을 것이다.

거의 대부분의 user들이 banking system을 사용하는 device가 본인의 PC 혹은 smart phone이고, 그 외의 device를 사용할 경우는 거의 없기 때문에, 불편함을 겪을 상황은 거의 없을 것이다. 만약 device를 추가로 등록하거나 변경할 경우에는 등록된 device 내에서 가능하도록 만들면 조금의 불편함 또한 감소시킬 수 있다.