컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 암호란 무엇인가?
- 저장 정보 암호화
- 전송 정보 암호화

암호

암호란 무엇인가?

사람들이 “암호”라는 단어를 사용하고, 암호를 이용해서 우리 자신과 정보를 보호하는 방법에 대해서 들어보았을 것이다. 하지만 암호 개념은 좀 헷갈리기도 하다. 추가로 암호는 모든 것을 보호할 수 없으며, 제약이 존재한다. 이 번달 호에서는 암호란 무엇인지 그리고 암호를 사용하는 이유, 그리고 암호를 실제 사용하는 방법에 대해서 간략히 설명한다.

객원 편집자

크리스토퍼 크롤리(@CCrowMontance; +ChrisCrowley)는 미국 워싱턴D C 지역에서 활동하는 컨설턴트이다. 크리스토퍼는 SANS의 모바일 기기 보안 및 윤리적 해킹(SEC575) 선임강사이며, 사고 대응팀 관리(MGT535) 과정 저자이다.

우리들은 금융 문서, 그림, 이메일 또는 의료기록과 같이, 우리가 사용하는 기기에 엄청나게 많은 민감 정보를 가지고 있다. 만약에 우리들이 기기 한대라도 분실한다면, 기기를 습득한 사람들이 기기에 있는 모든 민감 정보들을 볼 수 있다. 또한 온라인 뱅킹 또는 쇼핑시에는 온라인으로 민감 정보를 전송할 수 있다. 만약에 사이버 공격자가 우리의 온라인 활동을 모니터링하고 있다면, 금융 계좌 또는 신용카드 번호와 같은 모든 정보를 훔칠 수 있다. 암호는 이러한 상황에서 인가된 사람만이 정보에 접근하고 수정할 수 있도록 보호할 수 있다.

정보가 암호화 되어 있지 않는 것을 평문이라고 부른다. 이 말은 누구나 쉽게 정보에 접근하고 읽을 수 있다는 것이다. 암호는 평문의 정보를 비가독성의 정형화된 암호문으로 변경한다. 암호는 복잡한 수학적 연산 및 유일한 키를 이용해서 정보를 암호문으로 변경한다. 이 키를 이용해서 정보를 암호화하고 또는 해독한다. 가장 일반적인 키는 패스워드이며, 패스워드를 가지고 있는 사람만이 정보를 복호화할 수 있다. 암호화된 정보를 보호하기 위해서는 키를 보호해야 한다. 일반적으로 암호는 두 가지 방법으로 동작한다. 즉 컴퓨터에서 저장된 데이터와 같이 저장 데이터를 암호화하는 것과 온라인으로 전송되는 정보를 암호화하는 것이다.

저장 정보 암호화

저장된 정보를 암호화하는 첫 번째 목적은 컴퓨터나 모바일 기기들이 분실될 경우에 정보를 보호하기 위해서이다. 15년 전에는 이 문제는 크지 않았다. 왜냐하면 대부분의 컴퓨터는 크고, 무거웠기 때문에

암호

암호는 정보를 보호하기 위한 강력한 방법이지만 키 길이 비례한다.

컴퓨터를 이동하는 것이 어려웠기 때문이다. 요즘에는 많은 노트북이 굉장히 가벼워졌으며, 모바일 기기는 더 가볍다. 하지만 이러한 기기들의 성능은 뛰어나서 엄청난 량의 정보를 보유하고 있으나, 분실하기도 쉽다. 추가로 USB 또는 CD-ROM과 다른 모바일 미디어에도 같은 민감한 정보를 보유하고 있다. 일반적인 암호화 기법은 풀 디스크 암호화(FDE)라고 부른다. FDE는 시스템에 있는 모든 데이터를 암호화 한다. 또한 암호화할 것과 아닌 것을 결정하지 않아도 된다. 최근 대부분의 운영체제는 기본적으로 FDE 기능을 제공하고 있어 설정해서 사용만 하면 된다. 예를 들어 MacOSX에는 FileVault가 있으며, 윈도 일부 버전에는 비트로커(BitLocker)가 포함되어 있다. 만약에 컴퓨터에 FDE 기능이 있다면, 반드시 사용할 것을 권고한다. 추가로 모바일 폰에서도 내부 저장 매체에 대해서 FDE기능을 지원한다. 예를 들어 아이폰, 아이패드용 iOS 운영체제는 패스워드를 설정하면 자동으로 FDE 기능이 적용된다. 컴퓨터나 모바일 기기가 FDE 기능을 지원하는 지 알고 싶다면, 관련 회사로 연락해보면 된다. 개인용 컴퓨터는 컴퓨터 제조사에 연락하던지 아니면 온라인 설명서를 보면 알 수 있다.

전송 정보 암호화

정보가 전송 중일 때도 취약하다. 데이터가 암호화 되지 않으면 인터넷상에서 모니터링 되거나 캡쳐 될 수 있다. 이러한 이유로 인터넷뱅킹, 이메일 전송, 심지어 소셜 미디어 사이트 접속 시에도 민감한 인터넷 활동이 암호화 되어야 한다. 인터넷 전송 암호의 가장 일반적인 방법은 HTTPS 이다. HTTPS를 이용하면 브라우저와 웹사이트간의 트래픽이 암호화 되어있다는 것을 의미한다. URL 에서 https:// 또는 브라우저의 잠금 아이콘 또는 URL 주소창이 초록색으로 변하는 지 확인해봐라. 이렇게 표시되면 통신이 암호화되고 있다는 뜻이다. 또한 공개된 와이파이 네트워크를 연결 할 때는 가능하면 항상 암호화된 네트워크를 사용하는 것이 좋다. 마지막으로 이메일을 보내거나 받을 때, 이메일 클라이언트 프로그램이 암호화된 채널을 이용하도록 설정되었는지 확인해 보아라. 많은 이메일 클라이언트가 암호기능을 제공한다.

암호기능 잘 사용하기

어떤 형태의 암호를 사용하던 간에, 대부분 암호기능을 잘 사용하기 위해서는 다음과 같이 일반적인 조치가 필요하다.

암호

- 암호 강도는 키 길이에 비례한다. 키가 해킹 당하면, 데이터도 마찬가지로 해킹 당한다. 키를 보호해야 한다.
- 키로 패스코드 또는 패스워드를 사용하고 있다면, 패스워드를 길고, 안전하게 해야 하며, 분실하거나 잊어버리지 않도록 해야 한다. 만약에 잊어버리면 데이터는 거의 복구 할 수 없게 된다.
- 암호 강도는 컴퓨터의 보안에 비례한다. 만약에 컴퓨터가 해킹되거나 악성코드에 감염된다면, 해커가 암호기능을 우회할 수 있다. 그렇기 때문에 컴퓨터나 모바일 기기도 안전하게 관리해야 한다.
- 암호를 위해 다른 기능이 제공된다면, 항상 가장 강력한 방법을 선택하는 것이 좋다.

자세히 알아 보기

http://www.securingthehuman.org를 방문해서 OUCH! 뉴스레터를 읽어 보시고, 월간 OUCH! 정보보호지식 뉴스레터를 구독하십시오. 그리고 SANS 정보보호지식 솔루션에 대해서 좀 더 알아보시기 바랍니다.

한글판

본 문서는 한국의 ITL(http://www.itlkorea.kr)에서 번역하였습니다. ITL 은 미국 SANS 연구소의 한국 파트너로서 IT 거버넌스 및 IT 보안 분야의 최신의 지식과, 양질의 교육과 세미나를 진행하는 교육기관입니다. 추가적인 사항은 itl@itlkorea.kr 로 문의해주시기 바랍니다.

참고자료

맥 OSX Filevault:	http://support.apple.com/kb/ht4790
iOS 암호:	http://support.apple.com/kb/ht4175
안드로이드 암호:	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
윈도 암호:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
컴퓨터 보호:	http://www.securingthehuman.org/ouch/2012#december2012
패스워드 관리프로그램:	http://www.securingthehuman.org/ouch/2013#october2013

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, 번역: 진수희(ITL Inc.)