OUCH! | 2016 년 06 월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 암호란?
- 암호대상
- 올바른 암호 사용법

암호

암호란?

사람들이 "암호"라는 단어를 사용하고, 암호를 이용해서 우리 자신과 정보를 보호하는 방법에 대해서 들어보았을 것입니다. 하지만 암호 개념은 좀 복잡하며, 제약사항이 있다는 것을 이해해야 합니다. 이 번달 호에서는 암호란 무엇인지, 암호를 사용하는 이유, 그리고 암호를 실제 사용하는 방법에 대해서 간략히 설명합니다.

객원 편집자

프란시스코 보스코(@francibosco)는 연구원 및 프로젝트 관리자로서, 사이버범죄, 사이버보안 및 기술 오용과 관련된 프로젝트를 관리합니다. 그녀는 UN 국제범죄정의 연구원에서 근무하고 있으며, 테크앤로 센터 공동설립자입니다.

우리가 사용하는 컴퓨터 및 기기에 개인 문서, 그림, 이메일과 같은 엄청나게 많은 민감 정보를 가지고 있습니다. 만약에 우리들이 기기 한대라도 분실하거나 도둑맞으면, 기기를 습득한 사람들이 기기에 있는 모든 민감 정보들을 볼 수 있습니다. 또한 온라인 뱅킹 또는 쇼핑시에는 온라인으로 민감 정보를 전송할 수 있습니다. 만약에 누군가가 우리의 온라인 활동을 모니터링하고 있다면, 금융 계좌 또는 신용카드 번호와 같은 정보를 훔칠 수 있습니다. 암호는 이러한 상황에서 인가된 사람만이 정보에 접근하고 수정할 수 있도록 보호할 수 있습니다.

암호기술은 수 천년동안 존재해 왔습니다. 오늘날 암호는 훨씬 더 복잡하지만, 동일한 목적을 수행합니다. 즉 한 곳에서 다른 곳으로 비밀 정보를 보낼 때, 인가된 사람만이 정보에 접근하고 읽을 수 있도록 합니다. 정보가 암호화 되어 있지 않는 것을 평문이라고 부릅니다. 이 말은 누구나 쉽게 정보에 접근하고 읽을 수 있다는 것이다. 암호기술은 평문 정보를 비가독성의 정형화된 암호문으로 변경합니다. 오늘날 암호는 복잡한 수학적 연산 및 유일한 키를 이용해서 정보를 암호문으로 변경합니다. 이 키를 이용해서 정보를 암호화하고 또는 해독합니다. 대부분 이 키는 패스워드 형태입니다.

암호 대상

일반적으로 데이터 암호화는 두 가지 종류가 있습니다. 모바일 기기 또는 컴퓨터에 저장된 데이터를 암호화하거나, 이메일이나 메시지를 전송할 때와 같이 전송되는 데이터를 암호화하는 것입니다.

암호

저장 데이터 암호화는 컴퓨터나 모바일 기기가 분실되거나 도난 되었을 때 정보를 보호하는데 중요합니다. 오늘날 이러한 기기들의 성능이 좋고, 엄청난 양의 정보를 보유하고 있으나, 또한 분실하기 쉽습니다. 추가로 USB 또는 외장 하드디스크 와 같이 이동식 저장매체 등에서도 많은 민감정보를 보유할 수 있습니다. 디스크전체암호(FDE)기술은 시스템에 있는 모든 외부 드라이브를 암호화는 암호기술입니다. 즉 시스템의 모든 것을 자동으로 암호화하여, 암호화할 것과 아닌 것을 결정하지 않아도 됩니다. 최근 대부분의 운영체제는 기본적으로 FDE 기능을 제공하고 있어 설정해서 사용만 하면 됩니다. 예를 들어 Mac OSX에는 FileVault가 있으며, 윈도 일부 버전에는 비트로커(BitLocker) 또는 디바이스 암호기능이 포함되어 있습니다. 대부분의 모바일 기기에서도 FDE기능을 지원합니다. 예를 들어 아이폰, 아이패드용 iOS 운영체제는 패스워드를 설정하면 자동으로 FDE 기능이 적용됩니다. 안드로이드 6.0(마쉬멜로)부터는 하드웨어가 최소 표준을 만족하면 기본으로 FDE를 지원하도록 하고 있습니다.

암호는 정보를 안전하기 지키기 위한 강력한 기능이지만, 키 강도에 따라 암호의 강도가 결정됩니다.

정보가 전송 중일 때도 취약합니다. 데이터가 암호화 되지 않으면 인터넷상에서 모니터링 되거나 캡쳐될 수 있습니다. 이러한 이유로 인터넷뱅킹 및 통신에서 민감한 인터넷 활동이 암호화 되어야 합니다. 인터넷 전송 암호의 가장 일반적인 방법은 HTTPS 입니다. HTTPS를 이용하면 브라우저와 웹사이트간의 트래픽이 암호화 되어있다는 것을 의미합니다. URL 에서 https:// 또는 브라우저의 잠금 아이콘 또는 URL 주소창이 초록색으로 변하는 지 확인해보시기 바랍니다. 다른 예로 이메일을 보내거나 수신할 때, 대부분 이메일 클라이언트는 설정을 하면 암호기능을 제공합니다. 또 다른 전송 데이터 암호화 예로는, 아이메시지(iMessage), 위커, 시그널, 왓츠앱 또는 텔레그램같이 채팅 프로그램에서 사용자간 통신을 암호화하는 것입니다. 이러한 앱은 한쪽 시스템에서 다른 곳으로 전송중인 데이터에 제3자가 접근하는 것을 방지하도록 종단간 암호기술을 사용합니다. 이 말은 통신하는 양 끝 당사자만 전송 정보를 읽을 수 있다는 말입니다.

올바른 암호 사용법

암호기술 을 이용해서 데이터를 보호하기 위해, 암호기술을 정확하게 사용해야 합니다.

암호

- 암호는 키의 강도와 비례합니다. 누군가가 키를 추측하거나 접근한다면, 데이터에도 접근이 가능합니다. 즉 키를 보호해야 합니다. 만약에 우리가 키로 패스워드를 사용하고 있다면, 패스워드가 강력하고 유일한 것을 사용해야 합니다. 패스워드는 길수록 키를 깨기가 어렵습니다. 패스워드를 잊어버리면 안됩니다. 키가 없으면 정보를 복호화할 수 없습니다. 만약에 모든 패스워드를 기억할 수 없다면, 패스워드 관리프로그램을 사용해야 합니다.
- 암호 강도는 컴퓨터의 보안에 비례합니다. 만약에 컴퓨터나 기기가 해킹되거나 악성코드에 감염된다면, 해커가 암호기능을 우회할 수 있습니다. 그렇기 때문에 컴퓨터나 모바일 기기도 안전하게 관리하는 것이 굉장히 중요하며 그러기 위해서 안티바이러스, 강력한 패스워드 및 업데이트에 신경써야 합니다.
- 많은 모바일 앱 및 프로그램들이 데이터를 보호하기 위해 강한 암호기술을 제공하고 있습니다. 만약에 앱 또는 프로그램이 암호기술을 지원하지 않는다면, 다른 방법을 찾아보시기 바랍니다.

자세히 알아 보기

securingthehuman.sans.org/ouch/archives를 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

암호기술 설명:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
패스워드:	https://securingthehuman.sans.org/ouch/2015#april2015
패스워드 관리프로그램:	https://securingthehuman.sans.org/ouch/2015#october2015
악성코드란 무엇인가:	https://securingthehuman.sans.org/ouch/2016#march2016
테블릿 PC 보안:	https://securingthehuman.sans.org/ouch/2016#january2016

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley, 번역:진수희(ITL Inc.)