

## 컴퓨팅

## 인터넷뱅킹에도 쓰는 암호화 기술 보안 '우려'

SHA1 암호화 알고리즘 보안성 취약

손경호 기자

입력 : 2015.10.26.11:22

수정 : 2015.10.26.14:03

국내 주요 인터넷뱅킹 사이트를 포함해 대부분 암호화 통신을 제공하는 웹사이트가 지원하는 암호화 알고리즘(SHA1)이 이르면 올해 말부터 심각한 보안문제에 노출될 수 있는 것으로 나타났다.

SHA1은 해시값을 생성하는 암호화 알고리즘이다. 해시값이란 텍스트, 컴퓨터 코드 혹은 특정 메시지를 일정한 길이의 숫자, 영어대소문자로 표시되도록 암호화한 값이다. 이 값은 입력되는 정보에서 'coma(,)' 하나만 추가되도 완전히 변경되기 때문에 송수신자 간에 서로 믿을 수 있는 지를 검증하는 용도로 사용돼 왔다. HTTPS를 지원하는 웹사이트들의 경우 사용자PC/노트북에 설치된 웹 브라우저를 통해 이렇게 만들어진 해시값이 변하지 않았다는 사실을 확인하는 방법으로 해당 사이트가 안전한지 여부를 확인하는 과정을 거친다.

이 방법은 웹사이트에 대한 인증 외에도 실제 인터넷뱅킹, 소프트웨어 다운로드 등 여러가지 서비스에서 보안성을 확인하기 위해 쓰여왔다.



문제는 이러한 SHA1이 두 가지 서로 다른 정보를 입력했을 때, 같은 해시값을 만들어 낼 수 있는 시점이 온다는 것이다. 이를 악용한 공격을 '충돌공격(collision attack)'이라고 부른다. 이런 시점이 되면 더이상 SHA1을 활용한 해시값은 안전하다고 보기 어렵다. 앞서 MD5라는 암호화 알고리즘 역시 SHA1과 같은 용도로 활용됐었지만 이란을 대상으로 한 미국, 이스라엘 첩보기관이 수행한 사이버첩보활동에 악용된 '플레임(Flame)' 악성코드가 이러한 MD5에 대한 충돌 공격을 활용해 각종 정보를 수집하는데 악용됐다.(관련링크)

네덜란드 센트럼 위스쿤드&인포매티카, 프랑스 인리아, 싱가포르 난양공업대학 소속 연구원들은 현실세계에서 SHA1 암호화 알고리즘이 무너지는 시점이 올해 말로 앞당겨질 수 있다고 경고했다.(관련링크)

그래픽처리프로세서(GPU)를 활용하는 병렬컴퓨팅 기술이 발달하면서 훨씬 빠르고 적은 비용으로 SHA1에 충돌공격을 가할 수 있는 방법이 있다는 설명이다.

2012년 암호화 전문가로 유명한 브루스 슈나이어는 2015년에 SHA1 체계를 부수기 위해 70만 달러가 들지만 2018년에는 17만3천달러가 들 것이라고 예측한 바 있다.

그러나 이들 연구팀에 따르면 컴퓨팅 기술의 발전으로 인해 올해에는 7만5천달러~12만달러면 특정 웹서비스의 SHA1 체계를 무너뜨리는 공격이 가능하다고 주장했다.


때문에 SHA1을 사용해 왔던 주요 인증기관들은 내년 1월1일부터 이 방식을 사용중단하고 이보다 업그레이드된 SHA2 기반 인증서를 도입한다는 방침이다.

다행스러운 점은 SHA2 암호화 알고리즘을 적용한 웹사이트 수가 늘어나고 있다는 점이다. 암호화 기술 보급을 위한 비영리 단체인 트러스트워디인터넷무브먼트(TIM)에 따르면 전 세계 웹사이트 중 SHA1을 사용하는 곳은 약 24%로 많은 웹사이트들이 SHA2 체계로 전환하는 작업을 진행 중이다.(관련링크)

또한 구글 크롬, 모질라 파이어폭스는 2017년부터 SHA1 인증서를 사용하는 웹사이트에 대해서는 보안경고창을 띄우고 신뢰할 수 없는 연결이라는 사실을 알린다는 계획이다.

sontech@zdnet.co.kr 손경호 기자      저작권자 © ZDNet Korea 무단전재-재배포 금지

---

 **프린트**

 **닫기**