홈트레이딩 시스템에서 메모리 보안취약점 및 대응방안 제안

최민근*, 최민석*, 이동훈*
*고려대학교 정보보호대학원
e-mail:icon6@korea.ac.kr

Memory Security weak point and countermeasures of Home trading system

Min-Keun Choi*, Dong-Hoon Lee*, Min-Seok Choi*
*Graduate School for Information Security, Korea University

요 약

국내 주식거래 시장에서 사용되는 홈트레이딩시스템(HTS)은 PC와 인터넷만 연결되어있으면 누구나 쉽게 내려받아 이용할 수 있는 주식거래 프로그램이다. 집에서도 이용할 수 있는 장점 때문에 증권회사별로 HTS를 만들어 배포하고 있으며 사용자의 편의성과 효용성을 만족하게 하려고 다양한 HTS를 개발하고 있다. 하지만 사용자 편의성에 중심을 두다 보니 아직 보안에 대해 미흡한 점이 발견되고 있고 이러한 취약점에 대해 보완을 하고 있다. 따라서 본 논문에서는 아직 보완해야 할 부분이 많은 메모리 영역에서의 보안취약점에 대해서 알아보고 이를 막으려는 대응방법을 제시한다.

1. 서론

국내 주식거래 시장에서 사용되는 홈트레이딩시스템(HTS)은 PC와 인터넷만 연결되어있으면 누구나 쉽게 내려받아 이용할 수 있는 주식거래 프로그램이다. HTS는 이용자 편의성과 효용성을 높이기 위해 다양한 기능을 제공하며 증권회사는 다양한 사용자의 요구사항을 맞추기 위해 여러 가지 특수성을 지닌 HTS를 개발하여 공개하고 있다. 또한, 보안분야에서도 2008년 HTS에 대한 보안취약점 분석 논문[1] 시점과 비교해서 많은 관심을 보이고 있으며 금융감독원 역시 HTS 안정성 제고방안[2]과 같은 지침을 통해 인식을 같이하고 있다. 하지만 아직 많은 부분에 대해서 보안취약점이 나타나고 있다. 본 논문에서는 여러 가지 취약점 중 메모리에 대한 취약점을 분석한다. 본 논문의 구성은 2절에서 현재 HTS를 이용할 때 메모리에 나타나는 사용자 정보의 문제점에 대해서 알아보고, 3절에서는 분석방법에 관하서 기술하였으며, 4절에서는 평문으로 노출되는 정보에 대한 대응방안을 알아본다. 끝으로 5절에서 결론을 맺는다.

2. 현재 홈트레이딩 시스템 문제점

사용자가 HTS를 이용하여 주식거래를 할 때 필요한 인증정보는 ID, 비밀번호, 공인인증서 비밀번호이다. 이러한 인증정보는 암호화로 보호해야 하지만 메모리에 평문으로 노출되는 문제점이 있다. 그 밖에도 로그인 이후 이름, 주민번호, 이메일, 휴대전화번호와 같은 개인정보에 대해서 메모리에 평문으로 노출되는 문제점을 알 수 있다. 이러한 인증정보 노출에 대한 문제점은 메모리변조와는 다른 문제점이며 시큐어브라우저[3]와 같은 솔루션으로는 막을 수 없다.

(그림 1) HTS login 화면

3. 분석방법

HTS를 이용할 때 메모리에 인증정보가 평문으로 나타나는 문제점을 알아보기 위해 사용자 PC에 VMware를 설치하여 가상머신으로 실험환경을 만들었다. 사용자 PC와 가상머신은 <표 1>과 같은 사양이고 증권회사마다 각각 하나의 가상머신에서 실험하였고, 메모리 덤프 프로그램과 Hex editor은 win32dd.exe와 010editor을 사용하였다.

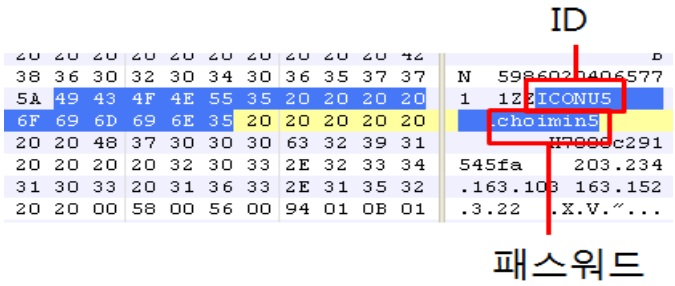
실험에 이용된 증권회사 HTS는 총 7곳이며 실험진행은 가상머신에 증권회사 HTS를 설치한 후 로그인 이전과 이후 각각 메모리 덤프를 추출하여 사용자 인증정보가 평문으로 노출되어있는지 비교하는 방식으로 진행하였다. 이

*본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원사업"의 연구결과로 수행되었음

실험에서 확인할 사용자 정보는 사용자 로그인에 필요한 정보와 주민등록번호와 같은 개인정보를 들 수 있다. 노출된 정보는 (그림 2)와 같이 나타나며. 로그인에 필요한 정보노출와 주민등록번호의 평문노출은 <표 2>로 정리하였다.

<표 1> 사용자PC와 가상머신으로 사용된 분석환경

	CPU	Memory	OS
사용자PC	Intel(R) Core(TM) i7-2620M CPU @ 2.70GHz	4GB	Windows 7 Enterprise K Server Pack 1
가상머신	Intel(R) Core(TM) i7-2620M CPU @ 2.70GHz	1GB	WindowsXP Professional Version Service Pack 3



(그림 2) 메모리에 노출된 정보

<표 2> 각 증권사별 노출된 정보

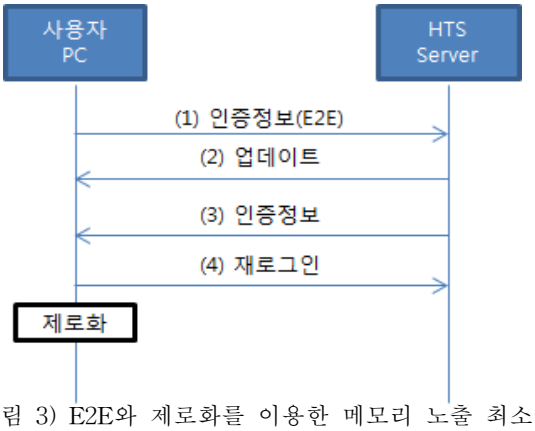
	ID	로그인 비밀번호	공인인증서 비밀번호	주민등록 번호
A증권	O	O	O	O
B증권	O	O	O	O
C증권	O		O	O
D증권	○	○	○	O
E증권	○	○	○	O
F증권	○	○	○	O
G증권	○	○	○	O

4. 대응 방안

HTS에서 인증정보 및 개인정보가 메모리에 노출되는 경우는 2가지로 나눌 수 있다. 첫째, 키보드 입력값이 그대로 노출되는 경우이고 둘째, 서버에서 보내오는 데이터가 메모리에 노출되는 경우이다. 키보드 입력값이 노출되는 첫 번째 경우는 E2E를 활용하면 평문 노출을 막을 수 있지만, 서버에서 보내오는 데이터는 E2E로 막을 수 없다. 따라서 E2E와 제로화를 함께 사용하여 메모리에 인증정보가 평문으로 노출되는 문제를 막는 방안을 제시한다.

(1) E2E와 제로화를 이용한 대응 방안

E2E(종단 간 암호화)를 사용함으로써 사용자 입력 데이터에 대해서 메모리에 평문으로 노출될 위험성을 없앨 수 있다[4]. 또한 제로화(Zeroization)를 통해 사용된 인증정보를 사용 후 즉시 '0 또는 1'로 덮어씌움으로써 인증정보가 메모리에 평문으로 나타나는 위험성을 줄일 수 있다[5]. 예를 들어 B증권의 경우 업데이트 진행 후 재로그인을 위해 인증정보를 사용자 PC로 보내는 과정을 수행한다. 이 과정에서 서버로 보내오는 데이터는 E2E를 적용할 수 없으므로 재로그인 후 제로화하여 인증정보를 지워야 한다. 이러한 제로화는 현재 사용되는 HTS를 크게 수정하지 않아도 적용할 수 있는 장점이 있다.



(그림 3) E2E와 제로화를 이용한 메모리 노출 최소화

5. 결론

증권거래의 대중화를 가져온 HTS이지만 보안상의 취약점은 여러 차례 나타났고 앞으로도 보완해야 할 점이 많다. 본 논문에서는 E2E와 제로화를 통해 로그인 후 메모리에 나타나는 인증정보의 흔적을 없애는 대안을 제시하였다. E2E와 제로화를 이용한다면 시스템구조 변경을 최소화하여 현재 메모리에 인증정보가 평문으로 남아있는 문제점을 해결할 수 있다. 하지만 제로화를 할 때 매우 짧은 시간 동안 메모리에 인증정보가 평문으로 노출되는 단점이 있다. 때문에 제로화는 위험요소를 줄이는 방법이다. 앞으로 위험요소를 제거하는 방법에 대한 연구가 필요하다.

참고문헌

[1] 이윤영, "홈트레이딩 시스템 서비스의 보안 취약점 분석 및 평가기준 제안" 정보보호학회논문지 제18권 제1호, 2008. 2

[2] 금융감독원 "증권, 선물회사 HTS 안정성 제고 방안 마련 2010. 5. 7

[3] 케이벤치, "안전한 인터넷 증권 거래 '시큐어 브라우저' 확산" http://www.kbench.com/hardware/?no=83820&sc=1 2010.5.3

[4] 금융보안연구원, "종단간(End to End) 암호화 적용 가이드" 2007

[5] NIST "Security Requirements for Cryptographic Modules" 1994. 1