증권거래 패킷의 암복호화와 통합보안관제 분석

오원겸* · 박대우**

*호서대학교

Encryption/Decryption and Enterprise Security Management of Stock Trading Packets

Won-Gyeom Oh* · Dae-Woo Park**

*Heoseo Graduate School of Venture University

E-mail : wgoh7147@naver.com · prof1@hoseo.edu

요 약

인터넷과 모바일 단말기를 이용한 금융거래가 활성화되면서, 인터넷과 모바일기기를 이용한 증권거래가 활성화되고 있다. 증권거래 관련 IT업무를 담당하고 있는 코스콤(증권ISAC)에서는 증권거래와 관련된 정보보안관련 취약점을 분석하며, 통합보안관제시스템을 가동하여 대응하고 있다.

온라인 증권거래는 개인정보보호법의 적용대상이며, 이와 관련 전산시스템들은 주요정보통신기반시설로 지정되어 있으나, 사용자 부주의, 해킹 등으로 인한 금융상의 피해가 예상된다. 이에 따라 증권거래 패킷의 암복호화, 통합보안관제 및 보안이벤트에 대한 분석을 통해 증권업무와 관련된 정보보안 분야의 주요 취약점에 대한 연구가 필요하다.

ABSTRACT

Financial transactions using a mobile terminal and the Internet is activated, it is a stock exchange enabled using mobile devices and the Internet. Koscom in charge of IT operations of securities transaction-related in (securities ISAC), to analyze the vulnerability of information security related to securities transactions, which corresponds to running the integrated security control system.

Online stock trading is a subject to the Personal Information Protection Act, electronic systems of related, has been designated as the main information and communication infrastructure to, damage financial carelessness of the user, such as by hacking is expected to are. As a result, research on the key vulnerabilities of information security fields related to securities business cancer decoding of the Securities and Exchange packet, through the analysis of security events and integrated security control is needed.

키워드

증권거래, 암호화, 복호화, 통합보안관제, 경보이벤트, 침해사고

Ⅰ. 서 론

대한민국은 2010년, 2012년 UN의 전자정부평가에서 1위를 차지하였으며, 이에 따라 온라인을 통한 경제적 활동이 보편화되면서 금융거래에서도 비중 추이가 점차 확대[1]되어 가고 있다.

증권거래에서도 인터넷과 모바일 기기를 통한 거래 금액이 계속 증가하고 있어, KOSPI 시장에서의 무선 매체를 통한 매도 규모가 2009년 20조원에서 2012년 약 89조원의 규모, KOSDAQ 시장의 경우 2009년 약 13조 5천억원에서 2012년에는 73조 7천억원[2]으로 성장하고 있다.

2013년 3월 20일 발생했던 언론기관(KBS, MBC, YTN)과 금융기관(신한은행, NH농협)들의사이버테러에서 해킹 공격에 따른 금융기관 및 투자자들의 피해 가능성이 있다.

㈜코스콤에서는 증권 IT업무를 총괄하면서, 온라인 침해사고대응을 위한 보안정보 공유를 위해

증권 ISAC을 구성하고, 관련 취약점, 침해사고 대응방안에 대한 관련 정보를 제공하고 있다.

증권관련 침해사고가 발생하면 CERT/CC를 통하여 증권업무의 침해사고에 대한 보안업무를 수행하고 있다.

증권관련 침해사고에 대한 보안성 강화와 국가 금융전산망에 대한 보안성을 확보하기 위해서는 증권거래 패킷에 대한 암·복호화 연구와 증권 온라인 침해사고 관련 보안 이벤트 분석 및 연구가 필요하다.

본 논문에서는 증권거래 패킷에 대한 암·복호화의 기술적 관점을 연구하고, 통합보안관제 및 주요 보안이벤트를 분석하여, 국가 자본시장의 주요 인프라중 하나인 증권 인프라에 대한 보안성 강화를 위한 기초 연구자료를 제공하고자 한다.

II. 관련연구

2.1 증권거래 패킷 구조

서버와 클라이언트 간 증권거래 패킷은 공통부와 계정계 및 정보계 영역 등으로 구성된다.

2.1.1 공통부 구조

증권거래 패킷의 공통부는 전문 길이, 전문 구분, 압축 구분, 암호화 구분, 데이터 옵셋으로 구성된다[3].

첫째 영역인 전문길이는 전문 전체(공통부, 업무별 영역, 데이터) 길이를 표시하는 영역으로 6Bytes로 구성된다.

전문 구분은 B:계정계, I:정보계 등을 표시하는 영역으로 1Byte로 구성된다.

압축 구분은 0:압축 안함, 1:LZO 등을 표시하는 영역으로 1Bytes로 구성된다.

암호화 구분 영역 또한 0:암호화 안함, 1:SEED-CBC를 표시하는 영역으로 1Byte로 구성된다.

데이터 옵셋은 3Bytes 구성되어, 입출력 데이터가 시작되는 위치를 표시하기 위해 사용된다.

2.1.2 계정계 구조

증권거래 패킷의 계정계는 서비스 코드(8Bytes), 이용사 번호(3Bytes), 사용자ID(16Bytes), 트랜잭션 ID(30Bytes), 공인IP(12Bytes), 사설IP(12Bytes), 처리지점번호(3Bytes), 지점번호(3Bytes), 단말분류코드(5Bytes), 단말번호(3Bytes), 언어구분(1Byte), AP 처리시각(9Bytes), 메시지코드(4Bytes) 등으로 구성된다[3].

2.1.3 정보계 구조

증권거래 패킷의 정보계는 윈도우 핸들(8Bytes), 접속클라이언트번호(4Bytes), 기관분류코드(2Bytes), 이용사번호(3Bytes), 상품구분(1Byte), 매체코드(2Bytes), 언어구분(1Byte), AUP번호(7Bytes) 등으로 구성된다[3].

2.2 암호화기술

암호화는 데이터 전송시 타인의 불법적인 방법에 의해 데이터가 손실되거나 변경되는 것을 방지하기 위해 데이터를 변환하여 전송하는 기술을 지칭한다. 암호화 기술에는 암호화 할 때의 키와 복호화 할 때의 키가 같은 대칭키 암호화 기술로 DES, AES, IDEA, RC5, Skipjack 등이 있으며, 암복호화시 서로 다른 키를 사용하는 비대칭암호화 기술로 디피와 헬만, RSA 등이 있다.

2.3 통합보안관제

통합보안관제(ESM ; Enterprise Security Management) 솔루션은 2001년부터 등장하여 다양한 이기종의 정보보호시스템의 보안이벤트를 수집하여 분석하고 일관된 정책으로 보안관리를 할 수 있도록 지원하고 있다[4].

2.4 보안이벤트 분석

보안이벤트를 분석하는 기술에는 실시간 보안이벤트 필터링 기술, 보안이벤트에 대한 상호연관분석 기술, 보안이벤트에 대한 시각화 분석 기술 등이 있다.

2.4.1 실시간 보안이벤트 필터링 기술

통합보안관제 솔루션은 보안시스템에서 생성하는 보안이벤트를 실시간으로 수집하여 분석할 수 있는 솔루션으로 이벤트를 종류별 또는 이벤트간 공통요소를 기반으로 분석이 가능하다. 즉, 동일 시간에 각종 정보보호시스템에서 동일한 공격대상 시스템에 대해 관련 보안이벤트가 발생하게 되면 이를 실시간으로 분석할 수 있다[4].

2.4.2 보안이벤트 상호연관분석 기술

보안이벤트 상호연관분석 기술은 ESM의 가장 핵심적인 기술로 다양한 보안이벤트 간의 상호연관 요소를 기반으로 침입을 추론하는 기술이며, 이에 대해서는 학문적, 상업적으로 활발한 연구가

진행되고 있으며, 관련 사례는 다음과 같다[4].

· 두 시스템간의 관계적인 요소 기반 분석
· 두 시스템간의 원인과 결과적 요소 기반 분석
· 세 시스템간의 원인과 결과적 요소 기반 분석

2.4.3 보안이벤트 시각화 분석 기술

보안이벤트 시각화 분석 기술은 네크워크상의 보안이벤트, 트래픽 정보들을 정보 시각화 기법을 이용하여 기존 텍스트 기반의 네트워크 정보시스템에서 찾기 어렵던 네트워크의 장애를 신속히 발견하여 신속하고 적적한 대처를 할 수 있게 해준다[4].

Ⅲ. 증권거래 패킷의 암호화

3.1 증권거래 패킷의 네트워크 구간 암호화

증권거래 패킷의 네트워크 구간(클라이언트 ~ 서버)에서는 사인코리아 암호화 모듈을 사용하여 로그인, 주문·체결, 입·출금, 조회 등 모든 전문을 암호화하여 송수신한다[5].

3.2 원장보관 데이터 암호화 기술

증권거래와 관련된 데이터를 보관하는 원장관리 서버에서는 고객 계좌 비밀번호를 사인코리아 암호화 모듈을 이용하여 암호화하여 저장 관리한다. 또한 로그인 비밀번호는 SHA-1 암호화 모듈을 사용하여 암호화하여 저장 관리한다[5].

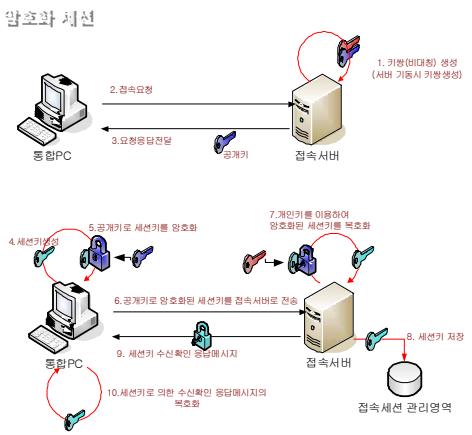

그림 1. 클라이언트와 서버간 암호화 세션

Ⅳ. 통합보안관제

4.1 통합보안관제 흐름

증권 ISAC에서는 증권계 50여개 기관의 보안이벤트를 3~5억건/일 실시간으로 전송받아 이글루시큐리티의 통합보안관리솔루션인 SPiDER TM을 통해 임계치 및 시그니쳐 작업을 통해 최적화하여 경보이벤트를 모니터링하고 있다.

증권계의 경우 경보이벤트는 2~3천건/일 발생하며, 1차 분석을 통해 이상 징후 이벤트라 판단되는 이벤트에 대해서는 심도있는 2차 연관 분석을 수행하여 침해행위라 판단시 대내외에 상황을 전파하고 관계기관과의 공조를 통해 금융전산 위기상황 대응반에서 복구 및 대응 조치를 취하게된다.

4.2 경보이벤트 분석

2013년 3월의 증권계 경보이벤트 분석을 통해 수집되어진 공격 유형을 살펴보면 침입공격이 1,613건, 정보수집(Scan)이 448건, 서비스거부(DoS)가 345건 발생[6]하였으며, 2013년 3월 20일 발생한 일부 언론기관 및 금융기관의 사이버테러 발생 이후인 3월 말부터 침입공격이 증가한 것으로 분석되고 있으며, 증권계로의 침입시도가 증가되고 있다.

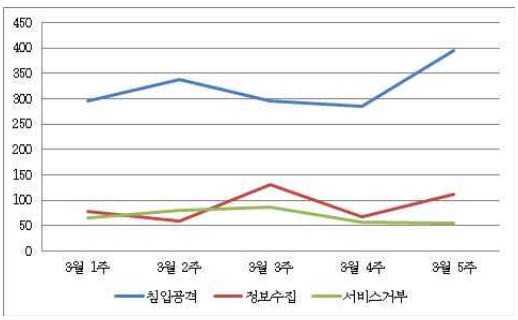

그림 2. 2013년 3월 증권계 주요 경보이벤트

4.3 침해사고 대응

㈜코스콤 증권ISAC의 CERT(Computer Emergency Response Team)팀에서는 증권계 관련 50여 기관의 침해사고 접수 및 처리를 통해 증권계 온라인 관련 침해 예방, 피해 복구 등의 업무를 수행하고 있다.

㈜코스콤에서는 온라인 공격유형을 하기의 표 2와 같이 분류하고, 표 3과 같이 온라인 공격에 대응하고 있다.

표 1. 사이버 공격 유형

구 분	공격 내용	공격 기법
해킹	◦ 웹 취약점을 이용하여 홈페이지 변조, 악성코드 유포, 자료유출 및 해킹지령 경유지 악용, 정보 절취 공격 수행 ◦ 비인가된 사용자가 전산시스템 및 전산망에 접근하여 데이터를 조작, 파괴, 은닉 또는 유출 ◦ 회원사 전산시스템을 위장하여 고객정보 유출 ◦ 응용 프로그램 취약점으로 전사 시스템 장애 발생	◦ 홈페이지 변조 ◦ 악성코드 유포지 악용 ◦ 자료유출 및 해킹지령 경유지 악용 ◦ 정보 절취
악성 코드	◦ 개인 및 금융정보 등의 자료 절취를 위해 시스템을 감염시키는 공격 ◦ 접근 권한이 없거나 접근 권한을 초과하여 내부 정보시스템 및 정보망에 접근하여 데이터를 조작·파괴·은닉 또는 유출	◦ 해킹 메일 발송 ◦ 피싱 사이트 접속
DDoS	◦ 특정 시스템을 대상으로 일시에 대량의 트래픽을 유발시켜 시스템의 정상 작동을 방해하거나 마비시키는 공격 ◦ 비정상정익 트래픽 유입으로 정보시스템의 정상적인 운영 방해	◦ 통신량 한계 초과 공격 ◦ 접속처리 한계 초과 공격 ◦ 홈페이지 부하가중 공격 ◦ 웹응용 프로그램 부하 가중 공격

표 2. 침해사고 대응 절차 및 내용

단계	대응 내용
탐지	◦ 경보이벤트 모니터링 ◦ 1차 이벤트 분석 ◦ 침해사고 여부 판단 ◦ 상황 전파
대응 및 조치	◦ 상황 보고 및 초동 대응체계 전환 ◦ 정보보호시스템 탐지 로그 분석 ◦ 유관기관 상황 보고 및 정보공유 ◦ 공격 트래픽, IP 등 차단정책 적용 ◦ 침해사고 분석 및 보고 ◦ 대응 조치 결과 보고
보고 및 완료	◦ 침해사고 결과 보고서 작성 및 보고 ◦ 참가기관 및 유관기관 결과 보고 ◦ 모니터링 강화 및 이력 관리

V. 결 론

본 논문에서는 증권거래 패킷의 암복호화, 통합 보안관제 및 보안이벤트에 대한 분석을 통해 증권업무와 관련된 정보보안 분야의 주요 취약점에 대한 연구를 하였다.

향후 연구로는 증권거래 패킷의 암복호화시 일어날 수 있는 취약점을 로그 분석하여 역추적하는 연구를 하여야 할 것이다.

참고문헌

[1] 행정안전부·방송통신위원회·지식경제부, “2012 국가정보화백서”, pp. 61, 2012년 8월.

[2] KRX 주식, 주식통계, 거래실적, http://www.krx.co.kr/m2/m2_5/m2_5_3/m2_5_3_1/JHPKOR02005_03_01.jsp, 2013년 4월.

[3] ㈜코스콤 PB시스템부, 차세대서비스 개발 헤더항목 정의, 2006년 11월.

[4] 최대수, 이용균, “ESM에서 보안이벤트 분석 기술에 관한 연구”, 한국컴퓨터종합학술대회 논문집, Vol. 34, Np. 1(D), 2007년

[5] ㈜코스콤 PB시스템부, “코스콤 PowerBASE 암호화 대상 내역”, 2010년 10월.

[6] ㈜코스콤 증권ISAC, “2013년 3월 증권계 주요 경보이벤트 분석 결과”, 2013년 4월.