情報保護學會論文誌
第20卷 第4號, 2010. 8

이용자의 금융거래정보 보호를 위한 확장 종단간(End-to-End) 암호화 기술과 보안고려사항

성 재 모[1†], 이 수 미[1], 노 봉 남[2], 안 승 호[2‡]
[1]금융보안연구원, [2]전남대학교 시스템보안연구센터

Extensional End-to-End Encryption Technologies to Enhance User's Financial Information Security and Considerable Security Issues

Jaemo Seung,[1†], Su-Mi Lee[1], Bong-Nam Noh[2], Seung-Ho Ahn[2‡]
[1]Financial Security Agency, [2]Chonnam National University System Security Research Center

요 약

종단간 암호화는 계좌 비밀번호 및 계좌번호 등 주요 금융거래정보를 암호화하여 이용자 PC에서부터 전자금융거래 서버까지 보호하는 것을 의미한다. 초기에 적용된 종단간 암호화는 이용자 PC내에 평문으로 존재하는 구간이 없어야 한다는 기본적인 보안요구사항을 만족하지 못하여 전자금융거래 시 여러 해킹기법에 의해 취약함이 발견되었다. 따라서 확장 종단간 암호화 기술은 이용자의 금융거래정보에 대해 기밀성 및 무결성을 제공하여 유출, 위·변조 등의 위협으로부터 보호하고 있다. 본 논문에서 확장 종단간 암호화 기술에 대해 살펴보고 금융회사에서 확장 종단간 암호화 기술 적용 시 고려해야 할 보안 고려사항에 대해 알아본다.

ABSTRACT

End-to-End(E2E) encryption is to encrypt private and important financial information such as user's secret access numbers and account numbers from user's terminal to financial institutions. There has been found significant security vulnerabilities by various hacking in early E2E encryption system since early E2E encryption is not satisfied the basic security requirement which is that there does not exist user's financial information on plaintext in user's terminal. Extensional E2E encryption which is to improve early E2E encryption provides confidentiality and integrity to protect user's financial information from vulnerabilities such as alteration, forgery and leakage of confidential information. In this paper, we explain the extensional E2E encryption technology and present considerable security issues when the extensional E2E encryption technology is applied to financial systems.

Keywords: Encryption, Financial system, Security requirement

I. 서 론

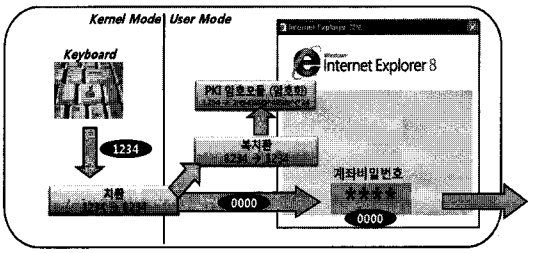
이용자 PC에 설치된 보안프로그램은 허락되지 않은 네트워크로부터의 침입 등과 같은 외부 해킹을 감지하여 이용자가 입력한 각종 개인 정보의 무단 유출 및 데이터 손상의 위협을 사전에 차단하는 역할을 수행한다. 이용자 PC에서 작동하고 있는 보안프로그램은 크게 키보드보안프로그램, PKI 응용프로그램, 백신프로그램으로 나눌 수 있다. 키보드보안프로그램은 키보드 키 입력 단계부터 이용자의 금융 정보를 보호

* 접수일(2010년 3월 2일), 수정일(2010년 5월 7일), 게재확정일(2010년 5월 12일)
† 주저자, sticom@fsa.or.kr
‡ 교신저자, shahn@chonnam.ac.kr

하며, PKI응용프로그램은 이용자 PC에서 금융서버까지 네트워크 구간에서 금융거래 정보를 암호화하는 역할을 담당하고 있다. 이외에 이용자 PC에서 트로이목마, 백도어 해킹프로그램, 특정 바이러스 등을 차단하기 위해 백신 프로그램이 동작하게 된다. 이와 같이 보안프로그램들이 동작됨에도 불구하고 이용자의 PC 단에서 보안상의 문제점들이 제기되고 있다. 이를 해결하기 위해 여러 가지 대응기술들이 제안되어 왔고 종단간 암호화(End-to-End Encryption)는 다양한 대응방식 중 하나의 기술이다. 종단간 암호화 기술은 키보드보안프로그램과 PKI 응용프로그램의 연동으로 이용자 PC 전 구간에서 금융거래 정보를 안전하게 전송하므로 외부 침입으로부터 보호할 수 있는 기술을 말한다. 결국 종단간 암호화를 통해 이용자의 금융거래 정보는 PC내에서 평문으로 존재하지 않으므로 전자금융거래 서버만이 금융거래 정보를 확인하게 된다. 종단간 암호화는 데이터 입력장치(키보드장치)로 입력된 값을 보호하는 키보드보안프로그램, 그리고 이를 암호화하는 PKI응용프로그램에 포함된 암호모듈로 구성되며 이러한 두 종류의 보안프로그램을 연결하여 종단간 암호화를 구성할 수 있다. 초기 종단간 암호화의 데이터 처리 방식은 암호화된 금융거래 정보를 이용자 PC에서 복호화하고 이를 다시 재 암호화하여 전송하는 방식이다. 즉 암호화된 키보드 입력값을 복호화하여 평문 형태로 존재하는 시점이 발생했고, 이 구간으로부터 보안위협이 발생할 가능성이 있다. 종단간 암호화의 기본 요구사항은 이용자 PC에는 암호모듈만이 존재하고 전자금융거래 서버는 복호모듈만이 존재하도록 설계하여 암호화된 데이터는 이용자 PC에서 복호화될 수 없어야 한다는 것이다. 따라서 본 논문에서는 초기 종단간 암호화의 문제점을 분석하고 초기 종단간 암호화 기술을 개선한 종단간 암호화 기술을 제시하여 이를 금융시스템에 적용할 때 고려해야할 보안 고려사항에 대해 기술한다.

II. 초기 종단간 암호화 기술

웹브라우저에서 이용자 계좌 비밀번호 보호를 목적으로 시작된 초기의 종단간 암호화 방식은 키보드보안프로그램에서 키보드 입력값을 치환 또는 암호화할 수 있는데 두 방식 중 어느 방식을 사용하느냐에 따라 종단간 암호화 기술을 분류할 수 있다. 즉 종단간 암호화 기술은 치환방식과 암호방식으로 분류한다. 각 방식의 특징과 동작 절차에 대해 알아보고 안전성에 대한 분석결과를 살펴본다.



〔그림 1〕 치환방식

2.1 초기 종단간 암호화

2.1.1 치환방식

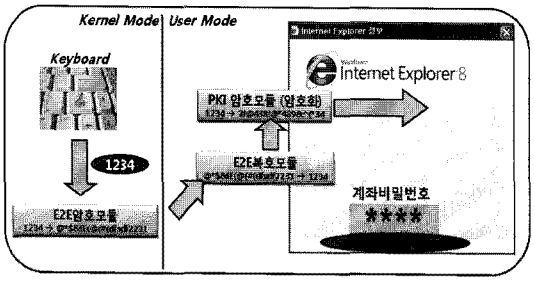
치환방식은 키보드보안프로그램에서 생성한 치환테이블로 이용자의 키보드 입력값을 단순 치환하여 보호하는 방식이다. 치환방식에 대한 세부 절차는 다음과 같다.

1. 데이터 처리 과정에 따라 이용자 입력값은 키보드보안프로그램에 의해 치환하여 별도 버퍼에 적재한다. 치환테이블은 랜덤 생성기에 의해 만들어져 키보드를 치환하는데 사용된다.(치환 테이블은 각 키보드 보안 프로그램 개발 업체마다 생성 방식에 차이가 있다)
   예) 이용자가 계좌 비밀번호 '1234'를 입력하면 키보드보안프로그램은 이를 치환테이블에 명시된 값 '8234'로 치환하여 메모리에 적재
2. 전송이벤트가 발생하면 치환값을 다시 평문으로 복치환한다.
   예) '8234'를 '1234'로 복치환
3. 복치환된 이용자 입력값을 PKI응용프로그램(암호화모듈)에 전송한다.
4. 마지막 단계로 PKI응용프로그램(암호화모듈)은 금융회사 서버 간에 공유된 세션키로 이용자 입력값을 암호화하여 금융회사 서버로 전송한다.

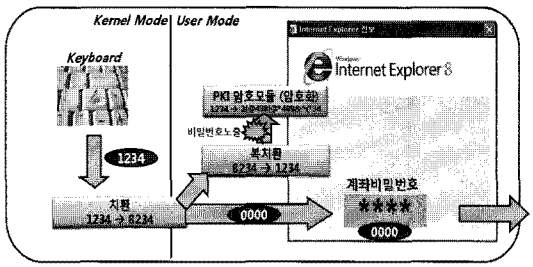
2.1.2 암호방식

암호방식은 키보드보안프로그램에서 자체 저장하고 있는 비밀키로 이용자 입력값을 암호화하여 이용자의 비밀정보를 보호하는 방식이다.

1. 키보드 입력 후 데이터 처리 과정에 따라 키보드 입력값은 종단간 암호화를 위해 키보드보안프로



〔그림 2〕 암호방식



〔그림 3〕 평문구간 존재로 인한 위협

그램에 포함된 E2E암호모듈을 로딩하여 이용자 입력값을 암호화한다.

예) 이용자가 계좌 비밀번호 '1234'를 입력하면 키보드보안프로그램의 E2E암호모듈에 의해 '@*$ &IE(@(#(dfsdf2231'로 암호화

2. 전송 이벤트가 발생하면 키보드보안프로그램의 E2E복호모듈이 로딩되어 암호문을 복호화한다.
예) 키보드보안프로그램의 E2E복호모듈에 의해 '@*$ &IE(@(#(dfsdf2231'는 계좌 비밀번호 '1234'로 복호화
3. 복호화된 이용자 입력값을 PKI응용프로그램(암호화모듈)에 전송한다.
4. 마지막 단계로 PKI응용프로그램(암호화모듈)은 금융회사 서버 간에 공유된 세션키로 이용자 입력값을 암호화하여 금융회사 서버로 전송한다.

2.2 안전성 분석

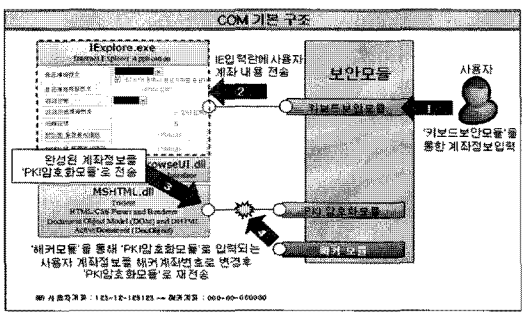
2.2.1 평문구간 존재

다양한 키로깅은 기본적으로 컨텐츠 및 주소창의 내용 등 웹브라우저 전반의 모든 데이터를 볼 수 있도록 인터페이스가 구성되어 있기 때문에 웹브라우저 윈도우 구조상 암호화가 지속되지 않으면 입력 데이터가 해킹될 여지를 제공할 수 밖에 없다. 이에 대응하기 위해 적용된 종단간 암호화는 키보드보안프로그램에서 키보드 입력값을 치환하거나 암호화하여 내부 버퍼에 적재한다. 하지만 PKI응용프로그램으로 전송하기 전에 복호모듈에 의해 평문으로 존재하는 구간(시점)이 존재하게 되고, 이는 종단간 암호화의 기본적인 요구사항을 만족하지 못한다.

2.2.2 COM 후킹의 가능성

개인용 PC에서 주로 사용되는 운영체제인 MS Windows에 주요 기능을 연결시키기 위한 공통 인터페이스(Component Object Model ; COM)는 보안업체에서 개발된 대부분의 PC보안 소프트웨어에서 이용하고 있다. 즉 일반 응용프로그램과 웹을 연결시키기 위해 제공되는 ActiveX는 COM모델인 확장성 및 편리성에 기초를 두고 있으며, 금융회사는 이용자 정보를 보호하기 위한 각종 보안프로그램에 ActiveX 기술을 이용하여 설치 및 운영되고 있다. 보안업체 또한 자사의 보안프로그램의 유지보수 및 이기종간(키보드보안프로그램, PKI응용프로그램 등) 상호 정보를 쉽게 교환하기 위한 수단으로 주로 사용하고 있다. 현재 주요 보안프로그램은 ActiveX 기술을 이용하여 구동되고 있고 데이터를 처리하는 함수는 상호 이기종간 데이터를 처리하기 위해 모든 인터페이스의 부모가 되는 IUnKnown 인터페이스를 참조한다.

IUnKnown 속성을 가진 함수는 특별한 제한 없이 다른 모듈에서 해당 기능을 호출하여 사용되도록 설계되어 있기 때문에 IUnKnown 속성을 가진 중요 함수로 유입되는 데이터 열람이 가능하게 된다. 이로 인해 각 보안프로그램에서 요구되는 높은 보안성이 적절치 않은 데이터 통신 방법으로 인해 이용자 정보가 노출될 수 있는 문제점을 가지고 있다. 초기 종단간 암호화는 치환 또는 암호화를 통해 키보드 입력값을 보호하고 있지만 이후 암/복치환 또는 암/복호화 모듈간



〔그림 4〕 COM 후킹

API를 이용하고 있다. 따라서 키보드 입력값을 보호하고 있는 중요 함수들이 IUnKnown 속성을 가지고 있어 이를 통해 타인(해커)는 치환/복치환 또는 암/복호화 함수로 유입되는 데이터가 유출될 가능성이 있다.

2.2.3 고정키 및 불안전한 키 공유 방식 사용

초기 종단간 암호화에서 키보드보안프로그램과 PKI응용프로그램은 고정키를 서로 공유하고 이를 이용하여 키보드보안프로그램은 키보드 입력값을 암호화한 후, PKI응용프로그램에 전송한다. 이 과정에서 키보드 입력값에 대한 보호를 위해 고정키는 키보드보안프로그램과 PKI응용프로그램에서 세션 단위로 갱신되어야 한다. 하지만 초기 종단간 암호화 방식은 키를 고정적으로 사용하고 있어, 안전하지 않은 종단간 암호화를 구성하고 있다. 고정된 키를 사용하는 경우, 암호문에 대한 평문공격이 가능하며, 키 공유(또는 전달)를 위해 사용되는 과정이 안전하지 않은 경우 (예를 들어 다른 정보와 키를 단순히 접합하거나 연산하는 경우 등) 또한 키를 쉽게 유추할 수 있다.

2.2.4 메모리 해킹 기법을 이용한 전자금융거래 정보 노출 및 위·변조

'07. 8월 공론화된 보안위협 기법으로 웹브라우저에 존재하는 메모리를 조작하여 이용자 금융거래 정보를 위·변조 하는 기법이다. 메모리 해킹 기법은 새로운 해킹 기법이 아니며, 주로 온라인 게임 어플리케이션을 해킹하기 위해 주로 사용되었던 기법이다. 앞서 언급하였듯이 웹브라우저 내로 유입된 정보에 대한 위·변조를 감지할 수 있는 보안프로그램이 존재하지 않음으로 이용자가 웹브라우저의 비밀번호 입력폼에 데이터를 기록하는 순간 웹브라우저 메모리정책에 의해 비어있는 메모리 영역구간에 데이터를 기록, 재사용하고 있으며 해당 값을 변경 또는 탈취하여 금융거래 정보를 위·변조할 수 있다. 이와 같은 기술 또한 널리 알려져 있는 기술로 현재 게임 분야에서 광범위하게 연구되어지고 있으며, 이와 관련한 해킹 전용 도구 및 기법이 광범위하게 알려져 있는 상태이이며 MS(Microsfot)사의 MSDN 사이트 등에서 제공하는 공개 API를 주로 사용하고 있으며, 윈도우 프로그래밍을 접한 초급자도 해당 취약점을 이용한 해킹 도구 제작이 손쉽게 이루어지고 있는 상태이다. 하지만 메모리 변조 기술은 프로세스 메모리 영역 전체를 대상으로 특정 문자열을 다른 문자열로 대치하는 기법임으로 복잡한 단계를 거치는 금융거래 단계에서 부분적인 취약점이 존재할 수 있으나, 복잡한 단계를 정밀하게 콘트롤하기에 다소 어려움이 있는 공격이다.

2.3 단계 별 위협 시나리오

2.2에서는 초기 종단간 암호화의 잘못된 설계에 의해 발생될 수 있는 위협에 대해서 살펴보았다. 이와같은 초기 종단간 암호화를 기반으로 설계된 시스템에서 이체 시 단계 별로 발생될 수 있는 위협에 관한 시나리오를 살펴본다.

1단계 이용자 신원확인을 위해 공인인증서 비밀번호 입력 시 해당 프로세스의 메모리 영역을 검색하여, 인증서 비밀번호 절취 가능

2단계 계좌비밀번호, 입금계좌번호 및 금액 등을 입력할 때 각종 프로세스의 메모리 영역 검색, html 폼 변경, IUnKnown Function 후킹 등으로 인해 계좌비밀번호를 절취하거나 타입금 계좌번호로 변경 가능

3단계 예비이체에서의 거래 내역을 확인하고, 보안카드번호 또는 OTP를 입력 시 웹브라우저 메모리 영역 검색, html 폼변경, IUnKnown Function 후킹 등으로 계좌비밀번호, 보안카드 번호, OTP 절취 가능

4단계 이체거래내역을 최종 확인하고, 이용자가 승인 시 이용자 신원 재확인을 위해 공인인증서 비밀번호 재입력 시 해당 프로세스의 메모리 영역 검색 및 IUnKnown Function 후킹하여 인증서 비밀번호 절취

III. 확장 종단간 암호화 기술

웹브라우저에서 이용자 비밀번호만 보호하는 것으로 목적으로 시작된 초기 종단간 암호화 기술의 안전성 및 예상되는 위협에 대해 살펴보았다. 본 절에서는 초기 종단간 암호화의 기술을 보완 적용한 확장 종단간 암호화 기술에 대해 살펴본다. 확장 종단간 암호화 기술은 이용자 PC에 키보드보안프로그램의 E2E암호모듈(키 이벤트 발생 시 암호화하는 모듈)만이 존재하고, E2E복호모듈(E2E암호모듈에 대응되는 복호화 모듈)은 전자금융거래 서버에만 위치되도록 설계되었으며 초기 종단간 암호화의 보호영역인 비밀번호 입력

〔표 1〕 확장 종단간 암호화 적용 필드

구분	보호영역 및 종단간(E2E)암호 방식 제공 여부(이프지PC단)				
	공인인증서 비밀번호	계좌비밀번호	보안카드번호 (또는 OTP)	이체계좌번호	금액
초기 종단간 암호화	해당사항없음	보호	보호	미보호	미보호
확장 종단간 암호화				보호	보호

부분에서, 입금계좌번호 및 금액입력부분 등도 보호되도록 확장하여 적용한 것이다.

3.1 확장 종단간 암호화

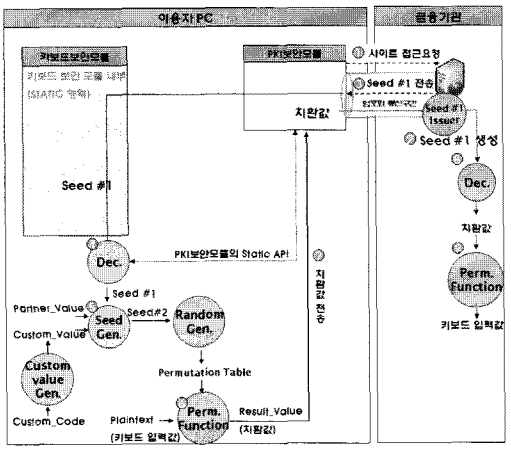
초기 종단간 암호화 방식의 문제점은 이용자 PC내에서 평문구간 존재, 고정키 사용, COM후킹의 가능성으로 분류할 수 있다. 이와 같은 문제점의 원인은 키보드 입력값을 암호화하기 위한 키를 키보드보안프로그램과 금융회사 서버 간에 직접 공유하지 않기 때문이다. 즉 금융회사에 전송되는 최종값은 이용자의 입력값이어야 하므로 PKI응용프로그램은 변경되지 않은 이용자의 입력값을 암호화하여 금융회사에 전송해야한다. 따라서 변경된(암호화된) 이용자의 입력값을 평문으로 만들기 위해서는 복호모듈이 필요하고 이때 사용되는 API, 고정키 등이 문제의 원인이 되고 있다. 이에 대한 문제점을 보완하면서 메모리 해킹을 통한 위변조에 대한 대응방식을 제안한다.

3.1.1 확장 치환방식

초기 치환방식의 문제점은 각 보안프로그램이 공유(또는 저장)하는 키로 인해 이용자 PC내 평문으로 존재하는 구간이 발생한다는 점이었다. 따라서 키보드보안프로그램과 최종 단계인 금융회사의 서버 간에 치환테이블을 공유하여 종단간에 암호화(데이터 변형)를 제공하는 방식으로 개선하고자 한다. 개선된 확장 치환방식은 키보드보안프로그램과 금융회사 서버가 치환 테이블을 공유하는 키공유 단계와 치환된 값을 암호화하여 금융회사 서버에 전송하는 전송단계로 나눌 수 있다.

❑ 키공유 단계

1. 서버는 치환 테이블을 생성하는데 사용될 Seed #1 생성
2. 서버는 암호화된 Seed #1(Enc_Seed #1)을 키보드보안프로그램의 영역에 전송
3. 키보드보안프로그램 영역에서는 정적(static) API를 이용하여 Enc_Seed #1을 복호화한 후 Seed #1을 획득
4. 치환 테이블 생성 과정
   - 키보드보안프로그램의 Seed Gen.(Seed #2 생성함수)에 Seed #1, Partner_value(해당 키보드업체의 유일값) Custom_value(해당 금융회사의 유일값)를 입력하여 Seed #2 생성
   - 랜덤 생성기(random generator)에 Seed #2를 입력하여 임의의 값을 생성
   - 치환 테이블 생성기(permutation table generator)에 임의의 값을 입력으로 치환 테이블 생성



〔그림 5〕 확장 치환방식(예)

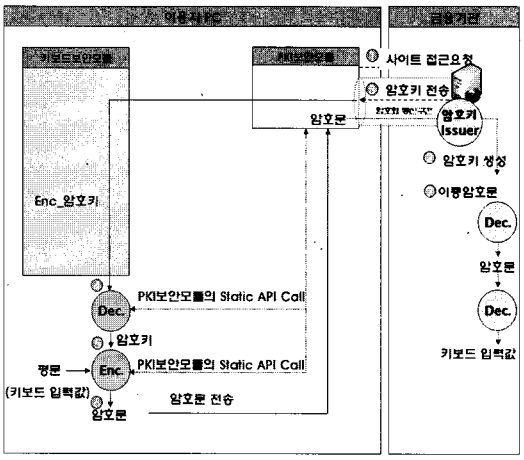
❑ 전송 단계

1. 키보드 입력값은 치환 테이블을 통해 치환값으로 매핑
2. 치환값이 암호화 모듈에 전송된 후, PKI응용프로그램은 치환값을 암호화하여 금융회사의 서버에 전송(웹브라우저의 "****"영역에는 임의의 숫자(dummy data, 예:1111) 전송)
3. 금융회사 서버는 복호화 과정과 복치환 과정으로 키보드 입력값인 평문 획득

다음은 확장 치환방식에 대해 가능한 유형을 도식화한 것이다. 다음은 키보드 입력값의 치환과정과 암호화된 Seed #1을 복호화하는 과정이 실행되는 확장 치환방식의 예를 나타낸다.

3.1.2 확장 암호방식

키보드보안프로그램과 최종 단계인 금융회사의 서



〔그림 6〕 확장 암호방식(예)

버 간에 암호키를 공유하여 종단간에 암호화를 제공하는 방식으로 개선하고자 한다. 개선된 확장 암호방식은 키보드보안프로그램과 금융회사 서버가 암호키를 공유하는 과정인 사전단계와 PKI응용프로그램과 금융회사 서버간에 공유된 세션키에 의해 재 암호화하여 금융회사 서버에 전송하는 전송단계로 나눌 수 있다.

❑ 키공유 단계

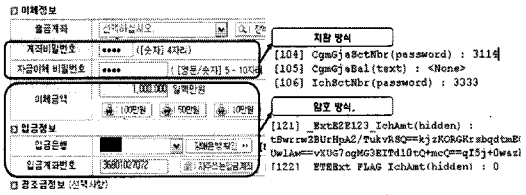
1. 금융회사 서버는 키보드 입력값을 암호화할 때 사용될 암호키를 생성
2. 금융회사 서버는 암호화된 암호키키(Enc_Session Key)를 키보드보안프로그램의 영역에 전송
3. 키보드보안프로그램에서 PKI응용프로그램의 정적 API를 호출하고 Enc_Session Key를 복호화하여 암호키 획득
4. 과정 후, 암호키는 금융회사의 서버와 키보드보안프로그램 간에 공유

❑ 전송 단계

1. 키보드보안프로그램에서 PKI응용프로그램의 정적 API를 호출하여 키보드 입력값을 암호화
2. PKI응용프로그램은 암호문을 이중 암호화하여 금융회사에 전송
3. 금융회사 서버는 이중암호문을 두 번의 복호화 과정 후, 키보드 입력값인 평문 획득

3.2 확장 종단간 암호화 기술 적용 형태

확장 치환방식과 확장 암호방식을 혼합하여 사용하



〔그림 7〕 입력폼별 적용된 확장 종단간 암호화 기술의 혼용형태

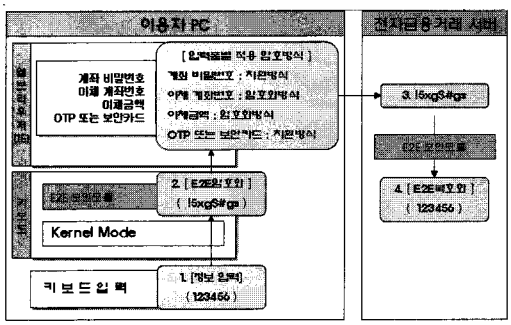
는 형태(혼용형태)와 확장 암호방식만을 사용하는 형태(단일형태)로 나눌 수 있으며 금융회사의 기존 시스템에서 활용 가능한 형태를 적용할 수 있다.

3.2.1 확장 종단간 암호화 방식의 혼용형태

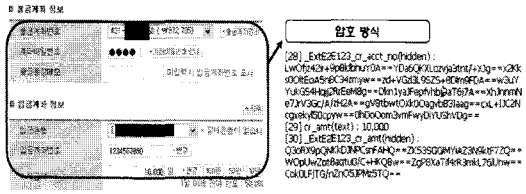
확장 치환방식과 확장 암호방식을 혼용하는 형태를 사용하여 계좌비밀번호 및 보안카드 비밀번호 입력에는 치환방식을 적용하고, 입금계좌번호 및 이체금액 입력부분은 암호방식을 적용하고 있다. 다음은 확장 종단간 암호화 기술이 적용된 영역을 분류하고, 기술 적용에 따라 생성된 데이터변형을 나타낸 것이다. 이용자 PC에서 E2E암호모듈이 구동되면서 웹브라우저 영역에는 암호문과 치환값이 나타나게 된다. 즉 기밀성을 제공해야하는 계좌비밀번호와 자금이체 비밀번호는 치환 테이블에 의해 치환값 '3114', '3333'으로 매핑됨을 볼 수 있고, 무결성을 제공해야하는 이체금액, 입금은행, 입금계좌번호에는 암호화가 적용되어 암호문이 html 히든필드속성에 저장됨을 볼 수 있다.

❑ 혼용형태의 구동절차

1. 키보드보안프로그램, PKI응용프로그램, 백신프로그램 등이 사전에 완전하게 설치되었다는 가정 하에 이용자는 키보드 입력장치를 통해 비밀번호 및 계좌번호 등 금융거래정보를 입력



〔그림 8〕 혼용형태 로직



〔그림 9〕 입력폼별 적용된 종단간 암호화 기술

2. 키보드 장치로부터 유입된 평문정보 E2E암호모듈에서 암호화되며 이렇게 암호화된 값은 웹브라우저의 html 히든필드속성에 저장 후 입력이 완료되면 이를 전자금융거래 서버로 전송
3. 전자금융거래 서버로 전송되어진 데이터는 E2E 복호모듈에 의해 암호 데이터를 복호화

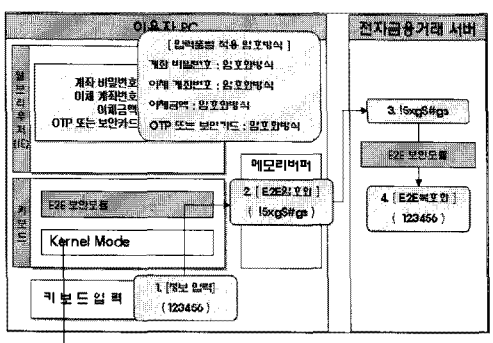
3.2.2 확장 종단간 암호화 방식의 단일 형태

단일형태의 경우 모든 입력폼에 암호화 방식만을 사용하는 경우에 해당한다. 즉 기밀성과 무결성을 제공하기 위해 모든 필드에 암호화 방식을 적용하여 다음과 같이 계좌번호, 계좌비밀번호 등 암호문 형태로 존재한다.

다음과 같이 절차에 따라 이용자 PC에서 E2E암호모듈이 구동되면서 웹브라우저 영역에는 암호문만이 나타나게 된다.

❑ 단일형태의 구동절차

1. 사전에 전자금융거래에 필요한 일련의 절차가 모두 완료 가정 하에 이용자는 키보드 장치를 통해 비밀번호 및 계좌번호 등 금융거래정보를 입력
2. 키보드 장치로부터 유입된 평문정보 E2E암호모듈에서 암호화되며 이렇게 암호화된 값은 웹브라우저의 html가 아닌 별도 메모리버퍼에 저장한 후 입력이 완료되면 이를 전자금융거래 서버로 전송
3. 전자금융거래 서버로 유입된 암호 데이터는 E2E복호모듈에 의해 암호 데이트를 복호화



〔그림 10〕 단일형태 로직

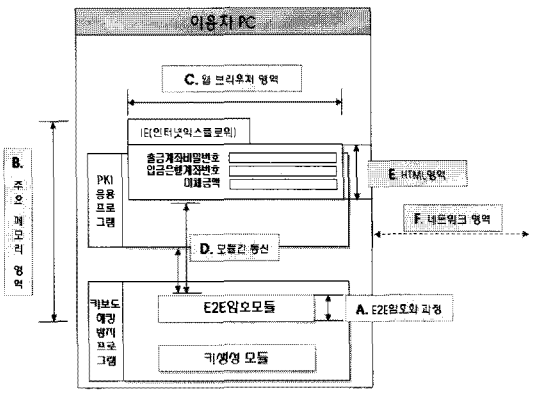
3.3 안전성

확장 종단간 암호화는 초기 종단간 암호화에서 가능한 위협을 방지하기 위해서 이용자 PC의 키보드보안프로그램(E2E암호모듈)과 금융회사 서버 간에 직접 암호키를 공유하는 시스템으로 되어 있다. 이는 주요 금융거래정보를 암호화한 후 그 암호문을 이용자 PC에서 복호화 과정없이 유지함으로 기밀성을 보장하게 된다. 이로 인해 PC에서 복호모듈을 제거하고 E2E암호키를 세션 및 페이지마다 갱신함으로써 COM후킹, 평문유출 등의 위협을 방지 할 수 있다.

또한 메모리 해킹을 통해 계좌번호, 금액 등을 변조할 수 있는 위협에 대해서도 계좌번호와 이체금액까지 종단간 암호화 대상을 확장함으로서 메모리 해킹으로 가능한 계좌번호와 이체금액의 위변조를 막을 수 있다. 확장 종단간 암호화는 계좌비밀번호, 보안카드 등 주요 금융거래정보에 대해서는 기밀성을 유지하고, 계좌번호, 금액에 대해서는 무결성을 제공함으로서 발생 가능한 위협에 대해 방지할 수 있는 시스템이다.

3.4 확장 종단간 암호화 시스템 설계 시 주요 보안고려사항

다음은 지금까지 살펴본 여러 가지 보안 위협을 감안하여 전자금융거래를 위한 확장 종단간 암호화 시스템 설계 시 고려 사항 및 설계 방법에 대해서 살펴본



〔그림 11〕 이용자 PC 보안 영역

〔표 2〕 주요 보안고려사항

과정 및 영역	주요 보안사항
A.암호화과정	A-1 E2E암호모듈 적용 이후 암호문에 대한 복호화 과정이 없어야 한다.
	A-2 E2E암호키를 안전하게 공유 및 갱신해야 한다.
	A-3 주요 금융 정보에 대한 암호화 값은 임의의 페이지 또는 동일 세션에서 재사용이 불가능해야 한다.
B.주요메모리	B-1 각 프로세스에 할당된 일부 또는 전체 메모리 영역에서 주요 금융거래정보에 대한 유출을 방지해야 한다.
	B-2 각 프로세스에 할당된 메모리 영역에서 주요 금융 정보에 대한 위·변조가 불가능하거나 위·변조 여부를 감지해야 한다.
C.웹브라우저	C-1 DOM(Document Object Model) 기술을 이용한 주요 금융거래정보 유출을 방지해야 한다.
	C-2 BHO(Browser Helper Object) 기술을 이용한 주요 금융거래정보 유출을 방지해야 한다.
D.모듈 간 통신	D. 모듈간 통신 데이터에 주요 비밀정보에 대한 유출을 방지해야 한다.
E.HTML	E. 확장 종단간 암호화가 적용된 입력폼이 위·변조될 경우 이를 감지하는 기능이 포함되어야 한다.
F.기타	F. 이용자 PC 및 네트워크 상에서 위·변조된 스크립트에 대해 감지 기능이 있어야 한다.

다. 확장 종단간 암호화가 적용된 시스템은 주요 영역을 E2E암호모듈에 의한 종단간 암호화 영역(A), 프로세스에 할당된 주요 메모리 영역(B), 웹 브라우저 영역(C), 이기종 모듈 간 통신 구간(D), HTML영역(E), 기타 영역으로 구분할 수 있다.

❑ A 암호화 과정

(A-1) 이용자 PC에서 키보드 입력값이 암호화된 후 복호화 과정을 수행하는 경우 키보드 입력값에 대한 종단간 암호화가 형성되지 않으므로 반드시 이용자 PC에서는 복호화 과정없이 서버로 암호문이 전송되어야 한다. 즉 이용자 PC내에는 E2E복호모듈이 존재하지 않아야 함을 의미한다. 이와 같은 성질을 만족하기 위해 E2E암호모듈과 금융회사의 서버 간에암호키가 공유되어야 한다.

(A-2) E2E암호모듈에 사용되는 암호키는 다양한 키공유 방식으로 서버와 공유하게 된다. 암호키를 공유할 때 고정키 및 취약한 암호알고리즘 사용 등으로 인해 E2E암호키의 유출 가능성이 있으므로 암호키 생성, 공유를 위해 권장되는 암호알고리즘 및 안전한 키 교환 프로토콜을 사용해야 한다.

(A-3) 금융거래정보에 대한 암호문이 재사용될 경우 비정상적인 거래가 발생할 수 있으므로 임의의 페이지 또는 동일 세션에서 재사용이 불가능하도록 매 페이지 또는 세션마다 암호키를 갱신하는 등 주요 금융 정보에 대한 암호문이 매번 변경되어야 한다.

❑ B 주요 메모리

(B-1) 거래 과정 중 암호키 또는 암호화 대상인 금융거래정보 등이 각 프로세스에 할당된 메모리 영역에 남아있어 결국 확장 종단간 암호화를 적용하지 않은 것과 동일하게 금융거래정보가 유출되는 상황이 발생될 수 있다. 따라서 확장 종단간 암호화를 적용할 때 기밀성을 요하는 주요 기밀정보가 메모리에 남지 않도록 설계해야 한다.

(B-2) 메모리 상에 존재하는 해당 암호문을 공격자가 원하는 암호문으로 위·변조하여 타계좌 조회 등 불법적인 거래가 가능하므로 암호키는 매 세션 또는 매 페이지마다 정상적으로 갱신되어야 하며 금융서버에서는 복호화 후 정상적인 계좌번호임을 확인해야 한다.

❑ C 웹 브라우저

(C-1) Html문서를 웹브라우저에 표시하기 위해 파싱 및 랜더링에 사용되는 mshtml컴포넌트는 DOM (Document Object Modeling)객체 및 BHO (Brower Helper Object)등에서 웹브라우저 이벤트 및 Html문서 속성 등을 제어할 수 있도록 설계되어 있다. 따라서 DOM에서 주요 금융거래정보가 유출되는 것을 방지하기 위해 암호화를 적용해야 한다.

(C-2) (C-1)과 같은 이유로 BHO에서 또한 주요 비밀정보가 유출될 수 있으므로 주요 금융거래정보의 필드에는 확장 종단간 암호화를 적용해야 한다.

❑ D 모듈 간 통신

(D-1) ActiveX으로 구성된 여러 모듈들은 모듈간에 데이터를 이동시키기 위해 사용되는 함수들이 존재한다. 이 때 사용되는 함수를 후킹하여 이동되는 주요 금융거래정보 및 암호키가 유출될 수 있으므로 암호화를 적용해야 한다.

❑ E HTML

(E-1) html 문서에 대한 무결성 검증의 부재로 인해 html 문서속성 변경 등으로 주요 금융거래정보가 유출되는 보안위협이 발생할 수 있으므로 확장 종단간 암호화가 적용된 입력폼이 위·변조될 경우 이를 감지하는 기능이 포함되어야 한다.

❑ F 네트워크

(F-1) 이용자 PC에서 스크립트 위·변조 검사 또는 스크립트에 대한 전체 암호화 기능을 제공하지 않아 네트워크 상에서 스크립트 위·변조가 발생한 경우 주요 금융 정보에 대한 노출 위협이 존재할 수 있으므로 이용자 PC 내 또는 금융회사 서버에서 스크립트 위변조에 대해 감지기능을 제공해야 한다.

❑ 확장 종단간 암호화 시스템의 제약 사항

확장 종단간 암호화를 적용하는 경우, 초기 확장 종단간 암호화에 비해 제약되는 몇 가지 사항이 존재한다. 첫 번째로 붙여넣기 기능, 마우스 드래그 기능 등과 같이 키 이벤트가 발생하지 않고 입력이 되는 경우 확장 종단간 암호화를 적용할 수 없다. 이유로는 입력 필드에서 키 이벤트가 발생할 때마다 키보드보안프로그램이 작동하게 되고 E2E암호모듈을 로드하여 암호화가 수행된다. 따라서 키 이벤트가 발생되지 않기 때문에 종단간 암호화를 수행하지 않는다. 두 번째 키보드 입력의 제약 사항으로 입력 필드에는 Backspace만 허용하고 그 외 방향키을 사용하지 못하게 된다. 키 이벤트가 발생하게 되면 순차적으로 한 캐릭터에 해당되는 암호문이 형성된다. 따라서 암호문 역시 생성 순서를 갖게 된다. 만일 방향키의 이동에 의해 중간 캐릭터를 변경한다면, 생성된 암호문에 오류가 발생하게 되고 이를 복호화한 서버에서 평문과 불일치한 값을 얻게 된다. 순차적으로 암호문을 생성해야 하기 때문에 입력 값 중 중간에 있는 캐릭터를 삭제, 삽입, 변경할 수 없어 방향키, spacebar 등의 사용을 차단하고 있다.

확장 종단간 암호화 기술은 이용자 PC에서부터 금융회사 서버까지 기밀성 및 무결성을 제공해야 하는 것을 목적으로 하고 있다. 따라서 전 구간에서 암호문 형태를 유지해야 하며, 설계 상의 문제로 주요 금융거래정보가 이용자 PC에 남겨지거나 재사용되지 않도록 해야 한다. 또한 E2E암호모듈에 사용되는 암호키 유출 방지는 이용자의 주요 금융거래정보에 대한 기밀성 유지를 위해 중요한 사항이다. 따라서 암호키는 세션마다 변경되어야 하며 암호키를 공유하기 위한 과정 중 평문으로 전송되는 구간이 존재하지 않아야 한다.

IV. 결 론

전자금융거래에서 발생되는 위협은 여러 가지 원인이 있고 이를 해결하기 위해 여러 가지 대응기술들이 제안되어 왔다. 종단간 암호화는 다양한 대응방식 중 하나의 기술이다. 종단간 암호화는 키보드 입력으로부터 금융회사의 금융거래 서버까지 이용자 금융거래정보를 보호할 수 있다. 초기의 종단간 암호화 기술은 금융거래정보 유출, COM후킹, 메모리 변조 등의 위협이 존재하여 이에 대한 대응 방안으로 확장 종단간 암호화 기술으로 개선되었고, 이를 적용한 입력 필드가 확대되었다. 하지만 보안위협에 대한 대응에도 불구하고, 역공학 기법을 이용한 해킹 등과 같은 다양한 위협의 가능성을 내포하고 있으므로 관련 업체의 지속적인 보안 강화가 필요할 뿐만 아니라 이용자 PC가 해킹되어 무력화되지 않도록 이용자의 보안의식을 향상시키는데 주력해야 한다.

본 논문에서는 전자금융거래 중 인터넷 뱅킹 거래 시 발생될 수 있는 위협에 대해 살펴보았고 이에 대한 대응기술 중 하나의 기술을 제안했다. 향후에는 개방형 모바일기반 뱅킹, 금융자동화기기, TV뱅킹 등 다양한 전자금융거래 별로 발생 가능한 위협을 분석하고 이를 방지하기 위한 보안기술에 대해 연구가 이루어져야 할 것이다.

참고문헌

[1] 금융감독원, "전자금융거래 보안 종합대책," pp. 1-81 , 2005. 9월.

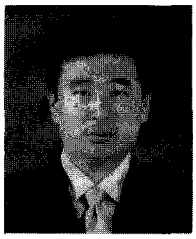
[2] 금융감독위원회, "전자금융감독규정시행세칙," pp. 1-15 , 2006. 12월.

[3] 금융보안연구원, "종단간 암호화 적용 가이드," pp. 1-70 , 2007. 7월.

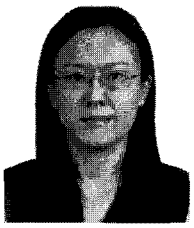
[4] 김인석, "전자금융 사고유형 분석을 통한 정보보호 정책에 관한 연구," 고려대학교 정보보호대학원 박사학위논문, pp. 5-48, 2008. 2월.

[5] 한국은행, "2009년 중 국내 인터넷 뱅킹 서비스 이용현황," http://www.bok.or.kr/contents/total/ko/boardView.action?menuNaviId=559&boardBean.brdid=67921&boardBean.menuid=559, 2009. 5월.

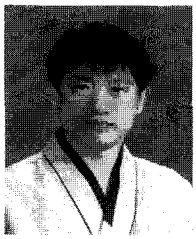
〈著者紹介〉



성 재 모(Jaemo Seung) 정회원
1993년 2월 : 스트븐스공과 대학원 전산학과 (석사)
2006년 2월 : 전남대학교 정보보호협동과정 박사수료
1993년 8월~2003년 8월 : 데이콤 정보보호기술팀 팀장
2003년 8월~2006년 10월 : KISA 인터넷침해사고대응지원센터 해킹대응팀 팀장
2006년 10월~현재 : 금융보안연구원 정보보안본부 본부장
〈관심분야〉 정보보호 관리체계, 포렌식, 컴퓨터와 네트워크, 모바일 보안, 금융보안 분야



이 수 미(Su-Mi Lee) 정회원
2003년 2월 : 고려대학교 정보경영공학전문대학원 (공학석사)
2004년 3월~2006년 8월 : 나사렛대학교 정보과학부 겸임교수
2007년 2월 : 고려대학교 정보경영공학전문대학원 (공학박사)
2006년 12월~현재 : 금융보안연구원 시험연구팀 선임연구원
〈관심분야〉 암호프로토콜, RFID인증시스템



노 봉 남 (Bong-Nam Noh) 정회원
1982년 2월 : KAIST 대학원 전산학과 (이학석사)
1994년 2월 : 전북대학교 대학원 전산과 (이학박사)
1983년~현재 : 전남대학교 전자컴퓨터정보통신공학부 교수
2000년~현재 : 리눅스 보안 연구센터 소장
〈관심분야〉 컴퓨터와 네트워크 보안, 정보보호시스템, 전자상거래 보안

안 승 호(Seung-Ho Ahn) 정회원
1981년 8월 : 전남대학교 대학원 수학과(이학석사)
1985년 2월 : 전북대학교 대학원 수학과(이학박사)
1987년 12월~1989년 12월 : 미국 미시간 대학 수학과 방문교수
1983년 5월~현재 : 전남대학교 수학과 교수
〈관심분야〉 암호학 분야