J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

임계 방식 기반 안전 비밀조각 공유 P2P 시스템 연구☆

Study on Threshold Scheme based Secure Secret Sharing P2P System

최 정 현1*
Cheong-Hyeon Choi

요 약

본 논문은 기업비밀 노출로 초래될 손실을 현격히 줄일 안전 비밀조각 공유 시스템을 제안한다. 본 연구 시스템은 중앙서버 방식이 아닌 효율적 P2P 분산 시스템을 제안한다. 최근 비트코인 유통 시스템도 역시 P2P 분산 방식을 사용하고 있다. 본 연구는 기능이 단순하고 확장성이 높고 전송 효율적인 토렌트 P2P 분산 구조와 그 프로토콜을 사용하여 토렌트 파일조각 대신 임계 샤미르(Shamir) 비밀조각의 보안 유통을 설계한다. 본 연구는 임계 샤미르 비밀조각 공유기법 (Threshold Shamir Secret Sharing Scheme)을 시스템에 적용하고. 동시에 다중 협동장치의 서명기법을 사용하여 안전하고 강력한 다중인증방식의 사용자 인증을 수행한다. 안전한 비밀 데이터 유통도 공개키로 암호화 교환된 임시키의 대칭암호방식의 효율적 암호화로 전송을 한다. 짧은 유효기간의 임시키는 세션 동안 생성되고 세션 마감후 소멸하므로 키 노출에서 안전하다. 특별히 본 제안한 시스템의 특징은 임계 분산기법을 효율적 토렌트 P2P 분산 시스템에 구조적 변경없이 효과적으로 적용한다. 동시에 본 시스템은 효율적인 임시키 대칭암호방식으로 비밀파일 유통에 기밀성을 보장하고 임시키는 공개키 암호방식으로 안전하게 교환된다, 본 시스템은 외부 유출 기기도 사용자로 동적 등록이 가능하다. 이 확장성으로 기밀성과 인증성을 동적으로 등록된 사용자에게도 적용할 수 있다.

☞ 주제어 : 샤미르 임계 비밀 조각; 협동인증; 쉬노르 암호기법;

ABSTRACT

This paper is to suggest the secure secret sharing system in order to outstandingly reduce the damage caused by the leakage of the corporate secret. This research system is suggested as efficient P2P distributed system kept from the centrally controlled server scheme. Even the bitcoin circulation system is also based on P2P distribution scheme recenly. This research has designed the secure circulation of the secret shares produced by Threshold Shamir Secret Sharing scheme instead of the shares specified in the torrent file using the simple, highly scalable and fast transferring torrent P2P distribution structure and its protocol. In addition, this research has studied to apply both Shamir Threshold Secret Sharing scheme and the securely strong multiple user authentication based on Collaborative Threshold Autentication scheme. The secure transmission of secret data is protected as using the efficient symmetric encryption with the session secret key which is safely exchanged by the public key encryption. Also it is safer against the leakage because the secret key is effectively alive only for short lifetime like a session. Especially the characteristics of this proposed system is effectively to apply the threshold secret sharing scheme into efficient torrent P2P distributed system without modifying its architecture of the torrent system. In addition, this system guaranttes the confidentiality in distributing the secret file using the efficient symmetric encryption scheme, which the session key is securely exchanged using the public key encryption scheme. In this system, the devices to be taken out can be dynamically registered as an user. This scalability allows to apply the confidentiality and the authentication even to dynamically registerred users.

☞ keyword : Shamir Threshold Secret Sharing; Schnorr Encryption Scheme; Collaborative Threshold Authentication

1. 서 론

최근 국내 경쟁력 있는 기업들은 경쟁력의 핵심 비밀이 국내외 경쟁업체로 불법적으로 유출되어 재산 피해를 경험한다. 특히 컴퓨터에 저장된 비밀자료의 불법적 노출은 원격에서 인터넷을 통해 은밀히 발생하지만 그 불법을 발견하고 법적 조치를 취하여 그 손실을 보상받기는 어렵다. 기업들은 비밀의 불법 노출은 사전에 예방하는 것을 최선이다.

먼저 기업은 비밀자료를 안전한 곳에 보관하고 그 다음 비밀자료 유통에서 권한 검증과 기밀성과 인증성을 보장하는 암호기능을 갖춘 시스템을 사용한다. 이와 같은

1 Dept. of MIS, Kwangwoon Univ., Seoul, 01897, Korea
* Corresponding author (chchoi@kw.ac.kr)
[Received 4 February 2022, Reviewed 7 February 2022(R2 6 May 2022), Accepted 25 May 2022]
☆ The present Research has been conducted by the Research Grant of Kwangwoon University in 2019.

맥락에서 새로운 시스템 도입에 과감한 투자를 하는 것이 현실이다. [1]

해외 사례로 중국 기업은 한국의 핵심 기술 확보하기 위해 여러 불법 통로를 이용한다. 예를 들면 경쟁기업의 사원을 경력직으로 채용, 협력사를 가장한 침투, 또는 경쟁기업의 정보기기를 탈취하는 등 다양한 방법을 가리지 않고 한국 경쟁기업의 산업기술을 습득하려고 한다.

최근 IT 기술발전으로 고용량 저장매체와 고속 네트워크를 이용하여 생산기술과 영업비밀 등 기업비밀을 해커가 원격 접속을 통해 불법 유출하고 있다. 사례를 보면 2012년에 국내 유출이 113건, 중국의 해외 유출이 27건에 달하고 이로 인한 누적 피해는 금액으로 5조 2,863억원에 달한 것으로 조사되었다. [1]

최근 조사에서 한국 기업들의 영업비밀 관리 예산의 주 용도가 컴퓨터 및 통신보안에 24%, 통제구역 설정 및 통제시스템 구축 및 유지에 19%로 나뉘고 있다. 다시 말해 외부로부터 컴퓨터 시스템에 악의적 해커 공격을 대비하고 불순한 내부자에 대한 영업비밀 접근통제에 초점을 맞추고 있다고 볼 수 있다. [2]

금융사가 포함된 3.20 해킹사태 이후로 금융위(원회)는 금융권의 보안사고를 막기 위해 인터넷과 내부망을 분리하는 망분리를 의무화하였다. 이에 금융위는 '금융전산 보안강화 종합대책' (7.11)을 마련하여 전산센터에 대해서 2014년 말까지 내부 업무망을 인터넷으로부터 원천 차단하는 물리적 망분리를 의무화하고 제2금융권은 2016년 말까지 완료하도록 하였다 [3].

1.1 비밀유출 방안의 취약점

비밀유출 방지를 위한 방안으로 금융위가 권고한 인터넷으로부터 망분리는 한국기업의 영업 및 업무환경으로 볼 때 업무처리에 필수적인 인터넷 사용을 제한하므로 생산성의 현격히 저하를 유발한다 [3].

망분리는 주로 논리적 망분리를 사용한다. 인터넷을 통한 외부 침입을 완전히 금지하는 물리적 망분리와는 달리 악의적 내부자는 망분리 내부망에 대한 원격 접근이 가능하므로 여전히 노출위험이 있어 100% 안전한 방안은 아니다.

보안에 민감한 기업들은 비밀을 중앙서버에 따로 저장하고 중앙서버를 물리적 통제구역에 위치시켜 물리적 통제를 강화하고 원격 접속은 허락된 PC만 접속 허락하는 보안방법을 사용하기도 한다.

원격 접근 보안은 이중인증을 사용하고 기업 비밀은 암호화 저장하고 유통한다. 비밀의 생성, 읽기, 변경은 오직 등록 애플리케이션만으로 제한하는 방법을 사용한다. 그럼에도 이런 보안조치도 현재 비밀파일 중앙서버 방식으로는 그 안전성을 100% 보장할 수 없다. 그 이유는 다음과 같다.

먼저 중앙서버 시스템은 무단인증 취약점 공격인 버퍼오버플로우나 벡도어 등의 공격으로 불법침입이 여전히 가능하고 현재 중앙서버는 아이디 패스워드 인증을 사용하면 패스워드 크래킹 공격이 가능하다. 중앙서버의 운영시스템은 완전한 패치관리가 되지 않으면 제로데이 공격 등이 가능하므로 불법적 침입이 이루어질 가능성은 여전히 있다. 무단 침입이 되면 그 사용자 권한만큼 비밀자료에 불법적 접근이 가능하므로 불법 노출을 원천봉쇄 하기는 어렵다.

1.2 연구방향

본 연구는 현재 기업비밀 불법유출을 가능하게 하는 네 가지 보안위험 요인에 대응하는 보안구조를 제안한다. 제안한 본 시스템의 특징은 첫째 중앙서버로 인한 유출 위험성을 낮추며, 단순성, 확장성 그리고 전송 효율성이 강점인 토렌트 P2P 분산 방식을 적용하였다. 둘째는 인증강화방안으로 협동인증을 채용하였디 [4][18].

(1) 유출 위험요인 회피 방안

첫째 요인은 내부직원의 부주의로 인한 인증정보 노출이다. 이는 사용자 인증과 추적 및 접근통제의 전체 정책을 무력화 할 수 있다. 비밀파일 보관 중앙서버 방식은 한 번의 무단침입으로도 전체 비밀파일이 무방비로 노출될 위험이 크다.

둘째 요인은 악의적 내부직원이 접근통제 정책의 취약점을 이용하여 그 내부직원보다 높은 권한의 사용자 권한을 도용하면 높은 등급의 비밀파일에 접근할 수 있는 노출 위험이다.

셋째 요인은 외부기업과 기술거래에서 외부로 가져가야 할 비밀파일을 담은 노트북이나 저장장치를 도난 당하여 외부로 누출되는 위험이다. 도난된 장치에 담긴 비밀파일은 중앙서버 방식보다 더 쉽게 해킹될 수 있는 위험이 있다.

넷째 요인은 버퍼오버플로우 등 인증을 무력할 수 있

는 소프트웨어 취약점이 있는 중앙서버에 비밀파일이 저장된 경우 노출위험은 더욱 크다. 이 요인은 보안 기능과 다른 문맥의 위험이므로 본 연구에서는 다루지 않을 것이다.

따라서 본 연구는 내부자까지 강력 인증하는 다중 협동인증을 적용하였고, 단일 중앙서버의 취약점을 피하여 외부로 소지하는 노트북도 사용자 노드로 등록할 수 있는 토렌트 P2P 분산 시스템의 확장성을 적용한 안전한 본 비밀파일 유통 시스템을 제안한다.

(2) 강력 협동인증 방안

현재 무단인증을 방지하기 위한 효과적이고 안전한 인증방식은 다중인증 (Multifactor) 방식이 선호된다. 그 중 이중인증은 사용자 아이디에 더해서 전화나 휴대기기로 추가 인증을 요청한다. 두 번의 인증 정보를 요구하는 방식이다.

본 연구는 투명한 다중인증 협동 임계 서명이라는 임계 인증서명 (Threshold Authentication Signature) 기반 방식을 사용하여 사용자 인증을 강화하였다. 이 협동서명 방식은 사용자 개인키를 사용자 협동 휴대장치와 컴퓨터에 분산하여 장치는 서명조각을 계산하고 사용자에 전송하면 서명조각을 합성한 서명정보로 인증을 수행한다 [14][16].

협동장치는 인증마다 다른 서명조각을 실시간으로 생성하므로 서명정보는 재사용으로 조작할 수 없다. 거짓 장치로 협동장치를 가장하고 악의적으로 서명조각을 임의 생성하는 경우 사용자 개인키 조각(share)이 없으므로 서명조각은 위조임을 알아낼 수 있으므로 조작은 불가능하다.

해커가 특정 협동장치를 불법 습득한다고 해도 그 내부 개인키 조각(share)을 사용하는 것을 불가능하다. 개인키 조각을 포함한 모든 인증 참여정보는 암호화 상태로 저장되어 있기 때문이다.

(3) 비밀자료 조각 분산방안

기존 비밀파일 중앙서버의 취약점을 해결하기 위해서 임계 비밀조각 공유기법 (Threshold Secret Sharing)으로 생성한 비밀조각을 P2P 기반 내부 유통망에 분산하는 방식으로 중앙서버 방식의 취약점을 피하였다.. 최근 비트토렌트 P2P 기반 파일유통 네트워크는 비트코인 등 강력 보안성이 요구되는 서비스에도 활용되고 있다는 것을 주목한다.

비밀파일에 대한 사용자 접근은 기업의 접근통제 정책을 통해서 사용자 등급을 따라 통제된다. 이 접근통제는 사용자 인증을 기반으로 사용자 등급과 권한이 결정되므로 접근통제도 인증 후 결정된다. 본 연구에서 접근통제보다 인증방식만 다루는 것은 동일한 메카니즘으로 결정되기 때문이다.

현재 중앙서버는 보안을 위해 사용자가 비밀자료를 생산하여 전송하면 접근등급과 권한정보를 결정하여 중앙서버에 등록되고 암호화 과정 등을 거쳐 보관한다. 그러나 중앙서버의 첫 결점은 파일유통에서 대역병목이 중앙서버에 집중되므로 성능저하 문제가 발생한다. 중앙서버는 비밀파일 암호화로 기밀성 유지 및 무결성 보장이 쉽지만 악의적 내부직원의 비밀접근으로 보안성 침해가 쉽다.

본 연구의 P2P 기반 비밀조각 분산 방식은 임계 비밀조각 분산방식으로 비밀파일을 분리하여 독립적 조각으로 만들고 분산망의 피어(peer)들이 보관함으로서 비밀자료 접근은 매우 까다롭고 힘들ㅁ므로 보안성은 높아진다. 분산 환경은 전송 병목현상도 없다.

1.3 연구목표

본 연구는 비밀파일의 안전한 보관과 유통을 위한 토렌트 P2P 분산망에 보안기능이 적용된 시스템 구조의 안전 비밀조각 공유 시스템을 제안한다. P2P 분산 시스템의 확장성과 전송 효율성의 장점을 사용하여 비밀을 분산하여 빠르게 공유할 자율적 피어(peer)들로 이루어진 분산 시스템이다.

특히 본 제안 시스템은 토렌트 P2P 네트워크의 프로토콜에 보안 요소를 강력하게 보장한 확장 프로토콜을 제안한다. 이 방식은 종단 피어들에 분산된 파일조각들을 사용자가 전송 요청하여 파일 전체를 다시 생성하는 빠른 효율적 시스템이다. 토렌트 P2P 시스템은 임계 비밀조각 분산에 아주 적합한 구조를 가진다. [15]

본 연구 시스템은 비밀조각 피어는 P2P 내부망에 있고 사용자는 외부 영업으로 이동이 가능하고 협동장치도 이동이 가능하지만 사용자는 비밀조각을 가진 P2P 내부망에 포함되지 않다. 사용자 컴퓨터나 협동장치가 도난되어도 그 속의 정보는 암호화되어 있으므로 비밀자료 노출에 안전하다 [15][16][17].

논문의 구성은 섹션 2에서 관련 연구, 섹션 3에서 본

연구가 제안하는 안전 비밀공유 시스템과 사용한 보안기법을 설명한다. 그리고 섹션 4에서 기밀성, 무결성, 인증성의 보안 안전성과 확장성을 논의할 것이다. 섹션 5에서 결론을 기술한다.

2. 관련 연구

2.1 망분리 기법

망분리는 기업, 기관 또는 단체 등의 내부망을 인터넷 공중망에 직접 연결이 되지 않도록 회선을 분리하는 방식을 말한다. 이 망분리는 그 구성에 따라 물리적 망분리와 논리적 망분리로 분류될 수 있고 논리적 분리방식은 다시 컴퓨팅 기반 방식과 서버 가상화 방식으로 나눌 수 있다 [5][6][7].

물리적 망분리 방식은 별도 분리된 두 망은 서로 다른 자원을 사용하여 동작함으로 가시적으로 두 망의 경계는 구분된다. 각 망마다 사용자 컴퓨터, 서버 그리고 통신장치 등이 별도로 분리되어 이것들이 이중으로 요구됨으로 안전성은 높지만 구축비용이 매우 높아진다. 사용자가 인터넷을 사용하려면 분리된 장치를 사용해야 하므로 업무 효율성이 매우 떨어지고 극히 불편하다 [5][6][7].

망분리 방안은 기업 내부 영업비밀 등 비밀자료가 외부망으로 불법 유출되는 통로을 원천적으로 막는 방안이지만 내부자에 의한 불법유출은 여전히 막을 수는 없다 [8].

2.2 토렌트 P2P 네트워크

토렌트 P2P 네트워크의 최대 장점은 단순함이다. 토렌트 사용자는 간단한 기능의 앱을 사용하여 피어에 파일 조각을 요청하고 응답받는 것은 HTTP Request와 Response 이다. 또 다른 장점은 높은 확장성과 운영방식이 단순하다는 점이다. 토렌트 P2P 엔티티의 구성과 기능은 단순하고 필요정보도 간단하다[10][12][18].

토렌트의 동작은 공유파일을 여러 파일조각으로 나누어 P2P 피어(peer)에 나누어 저장하고 그 파일조각의 위치 정보는 스웜프(swamp)라는 자료구조로 만들어진다. 스웜프는 공유파일 식별자로 그 해시값을, 파일조각을 소유한 피어주소 리스트를 담고 있고 이를 트래커(tracker)가 저장하고 관리된다. [13][18].

사용자가 토렌트 파일을 검색 웹에 요청하여 전송받는다. 토렌트 파일은 공유파일 식별 해시값과 트래커 URL 주소가 담겨 있다. 그리고 사용자는 트래커에게 공유파일의 조각을 가지고 있는 피어들의 주소 리스트를 요구한다. 요청하는 파일 해시값을 트래커-요청-메시지(Tracker request - HTTP request)로 담아 보낸다. 트래커는 공유파일에 해당하는 스웜프를 찾아서 트래커-응답-메시지(Tracker response - HTTP response)로 전달한다. 사용자는 리스트의 피어에 연결을 확립하고 파일조각을 전송 받는다 [13].

비트토렌트 프로토콜은 크게 핸드셔이크 단계, 파일을 가진 피어의 파일조각 정보를 받는 Have 메시지 단계, 파일조각을 요청하는 Request 메시지 단계. 그리고 피어로부터 해당 파일조각을 받는 Piece 메시지 단계로 나눌 수 있다 [13].

비트토렌트의 메시지 종류를 보면 해당 피어의 온라인 여부를 묻는 Keep-alive 메시지, Request에 답할 수 없다는 응답인 Choke 메시지, Choke 상태가 해지되었다는 응답인 Unchoke 메시지, 피어가 가진 파일조각 정보를 알리는 Have 메시지, 받고자 하는 파일조각의 인덱스와 Offset 정보를 알리는 Request 메시지, 실제 파일조각을 보내며 해당 인덱스와 Offset 정보를 담은 Piece 메시지 등이다 [13].

비트토렌트 피어(Peer) 종류는 전체 파일을 가진 시더(Seeder) 피어, 파일조각을 가진 리처(Leecher) 피어이다. 서버 피어는 공유파일에 대한 고유 식별자 해쉬값과 피어 주소를 관리하는 트래커(Tracker) 피어이다 [13].

이와 같이 비트토렌트 네트워크는 그 구성도 단순하지만 새로운 피어를 네트워크에 참여시키는 확장성도 좋다. 상호 통신은 사용자와 검색 웹, 사용자와 트래커 그리고 사용자와 피어 사이에만 집중된다. 따라서 임계 비밀조각 분산에 매우 적합하다. 인증성과 기밀성, 무결성을 시스템에 통합하기도 쉽다. 보안기능을 확장한 비트토렌트 네트워크는 매우 안전한 유통 구조와 프로토콜을 가지게 될 것이다.

한 예로 비트코인은 익명성과 분산화라는 두 가지 특성이 전자화폐 유통 시스템의 성공요인이다. 거래장부 분산에 비트코인 P2P 네트워크가 사용되었다는 것은 안전성도 보장된다는 의미이다 [10].

2.3 임계 비밀조각 분산

임계 비밀조각 기법 (Threshold Secret Sharing scheme)은 특정 비밀이 특정 컴퓨터에 저장되어 관리되는 경우 해당 컴퓨터의 여러 취약점을 공격받아 해당 비밀을 유출하는 것이 가능하다. 이를 방지하기 위한 임계 방식은 비밀을 조각내어 각 조각을 분산 네트워크 노드에 나누

어 저장하고 관리함으로서 특정 컴퓨터 내 조작을 유출해도 원래 비밀을 알아내기 어렵게 하는 방식이다 [11][14][15][16].

(k,n)-임계(threshold) 방식의 형식적 정의는 다음과 같다.

① 두 양수 k, n은 $k < n$을 만족한다.
② 비밀 S가 n개 조각으로 나뉘어 n명의 참가자에게 분산되어 저장되고 그 중 k명의 참가자 조각 전부를 가지고 비밀 S를 복원할 수 있다

(1) 비밀조각(Secret Share) 생성 및 분산

비밀조각을 생성하고 분산하는 샤미르 임계방식(Shamir Threshold Scheme)은 다음과 같다 [17].

① P: 참가자 집합 $\{P_1, P_2, \cdots P_n\}$; S: 비밀자료; D: 비밀 조각을 분산할 딜러(Dealer);
② D는 Z_p에서 $k-1$개 값 $a_1, a_2, \cdots a_{k-1}$을 무작위로 선정하고 $f(x) = S + \sum_{j=1}^{k-1} a_j x^j \bmod p$ 의 $k-1$차 다항식을 생성한다.
③ D는 비밀 조각 s_i를 $f(i) = s_i$로 생성하여 그 중 k개 조각을 $P_i \in U_c$, (여기서 U_c는 조각을 분배할 참가자 집합)에 보낸다.
④

(2) 비밀 복구 〔17〕

본 비밀조각을 모아서 비밀 S을 복원하는 과정은 Lagrange interpolation에 의해서 $f(0)$을 계산해 내는 과정이다. $(j, s_j)\, j \in U_c$ 만족하는 다항식은 동일하다.

① k개 비밀조각 $s_1, s_2, \cdots s_k$를 피어 $P_j,\ j \in U_c$에서 받는다.
② 다항식 $f(x) = \sum_{i=1}^{k} s_i \prod_{i \le j \le k,\, j \ne i} \frac{x-j}{i-j}$을 비밀조각으로부터 Lagrange interpolation에 의해 생성한다. $f(j) = s_j \prod_{i \le j \le k,\, j \ne i} \frac{j}{j-i}$를 계산한다.
③ 그리고 비밀 $S = f(0)$을 구한다.

2.4 (t,n)-임계 서명

(t,n)-임계 서명은 n개 참가자에게 서명조각을 분산시키고 그 중 t개 분산된 서명조각을 합성해서 보내어 검증자가 공개키와 Schnorr 방식으로 서명을 검증하는 방식이다. 임계 서명 방식은 중요한 거래에서 한 사람의 서명으로만 인증하는 것은 인증 우회 위험을 방지하는 방식이다.

인증 참가자들은 사용자가 분산한 개인키 조각으로 인증을 요청할 때마다 실시간으로 계산한 서명조각을 전송하여 사용자가 그 서명조각들을 합성하여 보내는 방식이다.

임계 서명은 다양한 인증/검증 알고리즘이 존재한다. 일반적 방식은 공개키 기반 서명에 사용될 개인키를 샤미르 비밀조각(Shamir Secret Sharing) 방식으로 개인키 조각으로 나누어 그 조각을 다중인증 참가자에게 분배하고 참가자는 그 개인키 조각과 실시간 선정 임의 정수로 계산한 서명조각을 사용자에게 전송한다. 사용자는 t개 참가자가 전송한 t개 서명조각을 가지고 최종 인증에 사용할 서명을 합성하여 검증자에게 보낸다 [17].

본 연구에서는 Schnorr 암호기법 기반 인증 방식을 사용한다.

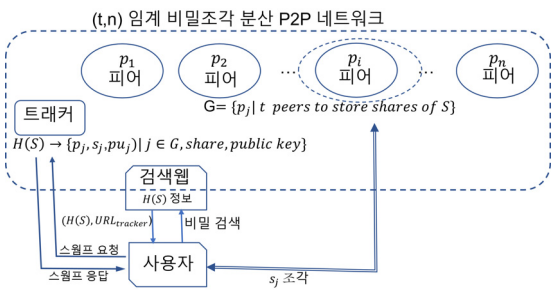
(1) Schnorr 서명방식(Signature Scheme) 〔14〕

본 방식에서 사용할 암호 파라메터는 다음과 같다.

① q : 큰 소수
② G : 차수 q의 그룹이고 이산대수 문제 기반
③ g : 그룹 G의 생성자
④ M : 메시지 공간
⑤ $H()$: $\{0,1\}^* \rightarrow Z_q$ 암호기반 해시함수

개인키 sk로 임의 정수 x, $1 \le x \le q-1$를 선정하고, 공개키 pk는 $y = g^x \bmod q$ 이다. 여기서 메시지 $m \in M$에 대한 인증과 검증은 다음과 같다.

① 서명함수 : $Sign(sk, m) \rightarrow (r, s)$
- 임의 정수 k for $1 \le k \le q-1$ 선정
- 서명조각에 사용할 $r = g^k \bmod q$ 계산
- 메시지 m와 r을 결합 $m \parallel r$ 생성
- 서명조각 $s = H(m \parallel r)x + k \bmod q$ 계산하고 최종 서명 (r,s)를 만든다



(Ffigure 1) p2p 기반 비밀파일 분산 구조도

② 검증함수 : $Ver(pk, m, s, r) \rightarrow 1/0$

- $g^s = g^{H(m \parallel r)x + k} = g^k g^{H(m \parallel r)x}$(1)
- $y^{H(m \parallel r)} r \bmod q$ (2)
- 위 (1), (2) 두 값이 일치하면 검증 완료

(2) Schnorr 임계 서명방식 [14]

개인키 x는 n개 조작 $x_i\,(1 \le i \le n)$을 전체 참가자에게 분배한다. t명의 임계 서명 참가자 P_i, $1 \le i \le t$와 중앙 게이트웨이 P_c가 다음과 같이 협동하여 서명을 생성하고 검증을 수행한다.

① P_c는 Lagrange 계수 $w_i = \prod_{\substack{j=1 \\ j \ne i}}^{t} \frac{j}{i-j}$ 계산하고 참가자 P_i에게 전송한다.

② 참가자 P_i는 임의 정수 k_i $(1 \le k_i \le q-1)$를 선정하여 $r_i = g^{w_i k_i} \bmod q$를 계산하고 P_c로 전송한다

③ P_c는 $r = \prod_{i=1}^{t} r_i \bmod q = g^{\sum_{i=1}^{t} w_i k_i} \bmod q$ 후 $h = H(m \parallel r)$ 계산하고 참가자 P_i에게 보낸다.

④ 참가자 P_i는 $s_i = hx_i + k_i \bmod q$ 계산 후 P_c에 전송한다. (개인키 조각과 임의 정수 사용)

⑤ P_c는 $s = \sum_{i=1}^{t} s_i w_i = \sum_{i=1}^{t} k_i w_i + hx \bmod q$ 계산 후 통합 서명 (r, s) 생성하고 검증자에게 전송한다

3. 안전 비밀공유 P2P 시스템

중앙서버 보안 취약점 제거

본 연구 시스템은 섹션 1.2에서 이미 언급한 것처럼 기업 내 영업비밀과 특허자료 등 비밀자료를 중앙서버에 보관하는 방식이 아닌 노출공격에 강력하게 방어하는 분산 방안을 제안한다.

이 노출공격의 두 가지 경로를 먼저 분석한다 [9].

첫째 경로는 기업 내부망에 침입 후 인증 우회 취약점을 이용하여 중앙 서버에 침입하는 잘 일려진 공격이다. 예를 들면 버퍼오버플로나 제로데이와 같은 알려진 취약점을 이용하여 이루어진다. 이는 전통적 해킹의 주 방식으로 취약점을 이용한 공격의 구체적 방법도 알려져 있다. 취약점 패치의 즉각적 설치는 보안에 중요하다.

그러나 내부자 아이디를 도용하는 경우나 내부자가 공모하면 이 공격은 근본적 방어가 불가능하다. 그러므로 보안을 위해서 비밀자료 저장은 중앙서버를 피하고 악의적 내부자 공모는 다중인증으로 봉쇄해야 된다.

본 시스템은 다중 협동인증을 사용하여 내부자가 공모한 경우도 악의적 내부자조차도 다중 장치들 전부를 제공해야 인증이 가능함으로 공모 실행은 원천적으로 매우 어렵다.

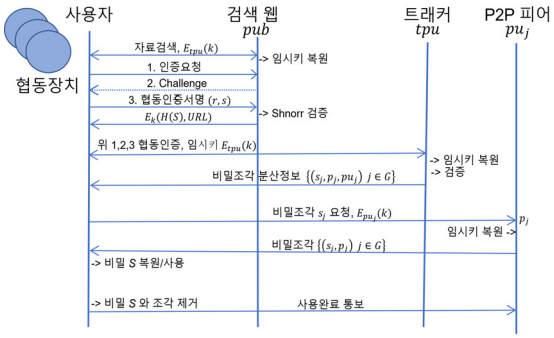
두 번째 경로는 이미 언급한 것처럼 중국과 기술영업에서 자주 발생하는 사고로서 기술영업을 목적으로 외부로 비밀자료를 가지고 갈 때 그 복사본을 담은 노트북이나 스마트 장치를 탈취하는 공격이다. 비밀지료는 노트북 등에 저장한 채 유출하는 것은 피해야 한다. 그러므로 강력한 다중인증 기반 P2P 시스템에 실시간 온라인으로 비밀자료에 접근해야 하고 비밀자료 사용 완료 후 비밀자료는 노트북 내부에서 파기되어야 하다.

본 시스템은 P2P 토렌트 분산 방식의 확장성으로 외부로 소지하는 노트북도 본 분산 시스템에 등록하여 암호화 및 다중인증의 보호를 받는다.

본 연구는 두 가지 취약 경로를 원천봉쇄하기 위해 다중 협동인증을 사용하고 비밀자료는 분산 P2P 피어로 분산하여 임시키 암호화 안전 전송으로 보호하는 방안을 제안하고 있다.

3.1 비밀조각 P2P 분산 시스템 구조

본 안전 비밀공유 시스템은 언급한 것처럼 임계 샤미



(Figure 2) 비밀조각 유통절차

르 비밀조각 (Threshold Shamir Secret Sharing) 공유방식으로 비밀자료를 여러 비밀조각으로 나누고 P2P 토렌트 피어들로 분산한다. 본 조각 분산 방식의 보안의 경력함은 일부 비밀조각으로는 원 비밀자료의 일부 또는 전체를 역으로 계산할 수 없다는 안전성에 기반한다. 임계 샤미르 비밀조각 공유방식은 임계 t개 조각 전체를 가져야 비밀을 복원할 수 있다. 또 비밀조각 분산은 토렌트 P2P 시스템의 파일조각 분산방식을 변경하지 않고 사용할 수 있으므로 본 연구 시스템을 토렌트 P2P로 구현하기가 매우 쉽고 그 프로토콜을 사용하기에 매우 적합하다.

위 그림 1은 본 연구 시스템 구조를 나타낸다. 본 시스템 아키텍춰는 토렌트 P2P에서 제안한 네 개 엔티티, 피어(Peer), 트래커(Tracker), 검색 웹(Web-site) 그리고 사용자(Client)의 구성을 그대로 사용한다. 본 안전 비밀조각 공유 시스템에서 각 엔티티의 역할과 그 보안기능을 다음과 같이 적용한다. 본 시스템에서 사용자는 일반 토렌트 시스템에서 언급하는 일반 사용자가 아니고 본 비밀분산 시스템에서 특정한 비밀파일에 접근할 수 있는 권한을 부여받은 개체들을 의미한다.

① 피어(Peer): 비밀파일 S의 비밀조각(Share)을 트래커로부터 분배받아 저장하고 사용자가 요청하면 전송한다. 각 비밀조각의 인덱스는 해시값 $H(S)$이다.

② 트래커(Tracker): 비밀파일 S을 생산한 피어 또는 사용자로부터 비밀자료를 받아서 샤미르 비밀조각 (Shamir Secret Sharing) 방식으로 n개 비밀조각을 계산할 $t-1$차 다항식을 계산한 후 임계 t개의 임의 피어(peer) 그룹 G를 선정하여 t개의 비밀조각들을 피어 그룹 G로 분산한다. 그리고 해당 비밀파일 S의 인덱스로 해쉬 $H(S)$을 계산하고 각 조각의 위치정보를 담은 스웜프(Swamp)를 생성한다, 그리고 비밀파일 인덱스와 파일정보를 검색 웹(Web)에 암호화 전송하여 각 사용자(Client)가 비밀파일 S를 검색 웹에서 검색을 할 수 있다.

③ 검색 웹(Web.) : 토렌트 웹처럼 비밀파일을 검색하도록 비밀파일 정보 $(H(S), URL_{tracker})$를 가지고 있다. 사용자가 검색 웹에서 비밀파일 정보를 사용하려면 협동 임계 인증 방식으로 검색 웹의 검증을 거쳐야 한다.

④ 사용자(Client) : 비밀조각을 피어에게 요청한다. 사용자는 협동 임계 인증 방식으로 검색 웹이 보내는 Challenge c를 서명하는 협동인증 절차로 검증되어야 한다.

3.2 비밀조각 사용 알고리즘

본 안전 비밀공유 사스템의 비밀파일 조각은 다음 샤미르(Shamir) 비밀조각 방식으로 계산된다. 사용 알고리즘은 생성, 분배, 공유, 복원, 폐기를 의미한다.

(1) 비밀파일 조각생성 기초 (섹션 2.3 참조)

샤미르 조각방식의 보안 파라메터는 다음과 같다.

피어 집합 $P=\{i \mid p_i$ 식별자$\}$, $|P|=n$ 는 P2P 네트워크 피어의 개수이다. 비밀자료 $S \in Z_q$, q 큰 소수이다. 비밀파일 S의 비밀조각 s_i는 $t-1$차 $f(x)$ 생성 후 $s_i = f(i) \bmod q, i = 1..n$로 계산된다 (섹션 2.3 비밀조각 생성 참조).

다항식 $f(x)$ 구성 방법은 반복하면 다음과 같다.

① 임의 정수 $a_j \in Z_q, 1 \le j \le t-1$ 선정

② $f(x) = S + a_1 x + \ldots + a_{t-1} x^{t-1}$ 생성

$f(x)$의 Lagrange Interpolation 방식으로 일대일 복원된 $g(x)$는 다음과 같다.(섹션 2.3 비밀자료 복구 참조)

① t개 비밀조각 집합 $L = \{s_i \mid 1 \le i \le t\}$선정

② $f(x)$의 복원 다항식 $g(x)$는 다음 Lagrange 기본함수 $g(x) = \sum_{j \in L} s_j \prod_{\substack{k \in L \\ j \ne k}} \frac{x-k}{j-k}$로 계산된다

③ 비밀자료 $S = g(0) = \sum_{j \in L} s_j \prod_{\substack{k \in L \\ j \neq k}} \frac{k}{k-j}$ 재구성

(2) 비밀조각 생성과 분배 절차

다시 요약하면 그림 1 시스템 구조에서 피어 또는 사용자가 비밀자료를 생성한다. 트래커는 그 비밀자료를 받아서 비밀조각으로 나뉘고 임의로 선정된 피어 리스트로 각각의 비밀조각을 분배한다. 트래커는 그 비밀조각 분배에 관한 정보를 담은 스웜프(Swamp)를 생성한다.

다음은 비밀조각 생성과 분배 알고리즘이다 (그림 2 참조).

① 생성 피어: 비밀자료 S 생성 후 트래커로 전송한다. 피어는 임의 정수로 임시키 k를 생성하여 등록 과정에서 받은 트래커 공개키 tpu로 암호화 $E_{tpb}(k)$ 하고 비밀자료도 임시키 k로 암호화 $E_k(S)$ 하여 전송한다.

② 트래커 :

- 비밀조각 분배 피어 리스트 G를 선정
- 비밀조각 $(s_j \, j \in G, |G| \geq t)$ 생성 후 비밀조각 s_j을 G의 p_j로 피어 임시키 k로 암호화 $E_k(s_i)$ 전송
- 비밀 S 인덱스 해시값 $H(S)$ 계산 후 S의 스웜프 $L = (H(S), (p_j, s_j, pu_j) \, j \in G)$을 구성한다. 여기서 공개키 생성은 임의 정수 pr_j를 선정하고 $pu_j (= g^{pr_j} \bmod q)$을 계산, 해당 피어 p_j의 공개키로 사용한다. 사용자가 임시키 k를 피어에 보낼 때 공개키 암호화는 $E_{pu_j}(k)$이다.
- 비밀자료 설명 정보를 검색 웹에 $H(S)$와 파일 설명을 임시키 암호화 전송하고 생산 피어에게 처리 완료를 통보하면 S를 제거. S의 검색 웹에서 공유를 시작한다

(3) 비밀조각 공유 및 복원 그리고 폐기 절차

본 안전 비밀조각 공유 시스템은 중앙서버가 아닌 P2P 피어에 기업의 모든 비밀파일을 토렌트 알고리즘으로 P2P 피어에 분산한다.

다음 그림 2는 본 안전 비밀조각 공유 시스템의 비밀자료 공유 절차를 보여준다. 사용자와 검색 웹과 트래커와 통신은 각각 공개키 pub와 tpu로 임시키 k는 공개키 암호화 $E_{pub}(k)$로 교환한다. 다음 절차를 가진다.

① 검색 웹은 토렌트 웹과 동일하다. 단 비밀자료는 강력한 협동인증이 검증된 사용자에게만 비밀자료 정보를 제공한다. 비밀자료 S는 인덱스 $H(S)$로만 식별되고 검색 웹의 비밀자료 정보는 $(H(S), \, tid)$ (여기서 트래커-URL가 tid)로 구성된다. 검색 웹은 이 정보를 $E_k(H(S) \parallel tid)$로 보낸다.

② 사용자는 비밀조각 분산정보 $(s_j, p_j, pu_j) \, j \in G$를 트래커에게 요청한다. 이 때 트래커와도 임시키 k를 암호화 $E_{tpb}(k)$ 교환하고 협동인증을 검증한다. (pu_j: 피어 p_j의 공개키)

③ 트래커는 비밀자료 S 인덱스 $H(S)$로 검색하여 스웜프 $L = (H(S), (s_j, p_j, pu_j) \, j \in G)$를 시용자에게 임시키 k로 $E_k(L)$ 암호화로 전송한다. (pu_j: 피어 p_j의 공개키)

④ 사용자는 스웜프 L를 복호하여 비밀조각을 가진 피어 p_j에게 비밀조각 s_j 전송요청을 임시키 k로 암호화하여 보낸다. 그리고 피어 공개키로 임시키를 $E_{pu_j}(k)$ 암호화로 전송한다. 리스트 G 내 모든 피어에게 비밀조각 요청을 반복한다. 사용자는 $s_j \, j \in G$를 사용하여 비밀자료 S를 복원하고 사용자 장치에는 $E_k(s_j)$, $E_k(S)$로 암호화 저장된다.

⑤ 사용자가 비밀자료 사용을 마치면 트래커에게 사용완료 통보를 한다. 그리고 모든 $E_k(S)$, $E_k(s_j) \, j \in G$를 사용자 장치에서 삭제한다.

⑥ 트래커는 비밀자료 노출을 방지하기 위해 일정 시간 사용완료 통보를 받지 못하면 기존 비밀조각을 재구성하여 불안전 비밀조각을 무효화 하여 노출을 방지한다.

(4) 비밀조각 관련 보안성

토렌트 P2P 프로토콜은 파일조각을 암호화 전송하지 않지만 본 안전 비밀조각 공유 시스템은 비밀조각의 전송이 암호화로 보호된다. 사용자는 검색 웹과 트래커와 통신하기 위해서 사전 등록이 되어야 한다.

특히 원격 접속으로 비밀자료를 전송받는 사용자는 사용권한 설정과 함께 검색 웹의 공개키 pub와 트래커의 공개키 tpu를 사전 교환 후 사용해야 한다. 비밀공유 안전성은 임시키 k를 공개키로 암호화하여 안전하게 전달한다. 사용자는 임시키 k 전달이 완료된 후 검색 웹과 트래커와 통신할 수 있다.

위 그림 3에서 보면 사용자는 임시키 $k \in Z_q$를 임의 선정한다. 공개키로 암호화한 임시키 k는 검색 웹과 트래커는 자신의 개인키로 임시키 k를 복원하여 비밀정보 전송에 사용한다.

임시키 교환 및 암호화 전송절차는 그림 2의 협동인증 부분으로 대표되며 그를 확대하면 임시키 교환을 포함한다. 상세한 졸차는 그림 3에서 기술되고 있다. 비밀조각 관련된 정보는 노출방지를 위해서 임시키 암호화로 전송된다.

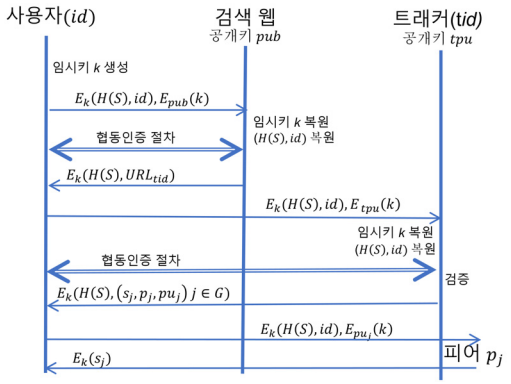
3.3 임계 협동장치 다중인증

본 안전 비밀조각 공유 시스템에서 안전한 협동인증은 특별히 외부로 비밀을 유출하여 영업을 하는 경우 다중인증으로서 비밀자료를 보호하기 위한 임계 인증 프로토콜을 사용한다.

사용자가 인증을 위한 서명을 생성할 때 협동장치가 서명조각 생성에 참여하는 방식이다. 협동장치는 사용자 등록 컴퓨터, 태블릿 등 계산능력을 갖춘 휴대장치이다.

(1) 사용자 협동장치 등록

사용자의 협동인증에 사용할 협동장치는 사전에 등록되어야 하고 등록한 사용자에게는 트래커가 접근권한을 부여한다. 사용자가 검색 웹이나 트래커에 인증요청을 보내면 접근권한을 확인한 후 합당한 시용자이면 Challenge c를 사용자에게 전송한다. 이 Challenge를 사용자는 협동장치로 보내 협동인증에서 사용된다.



(Figure 3) 임시키 암호전송을 포함한 협동인증

(2) Schnorr 인증 기초 (섹션 2.4 참조)

사용자가 서명을 생성할 때 각 협동장치는 독자적 임의 정수로 임시 개인키를 생성하여 Challenge c를 포함한 서명절차를 수행한다.

협동인증의 암호 파라미터는 큰 소수 q, 차수 q 그룹 G, 그룹 생성자 g, Challenge c의 메시지 공간 $c \in M$, 해시함수 $H(c): \{0,1\}^* \rightarrow Z_q$ 등 이다.

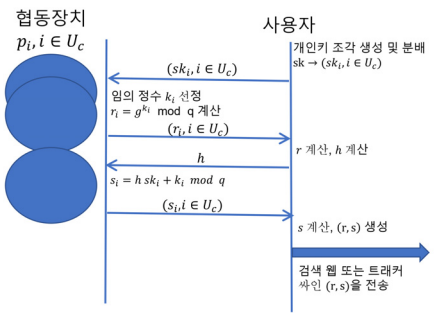
사용자 협동장치는 독자적으로 임의 정수 $x \in Z_q$를 임시 개인키로 사용한다. 그 공개키는 Schnorr 서명방식 (Authenticate Scheme)으로 계산하여 $y = g^x \bmod q$ 이다. 기본 서명생성 및 검증 알고리즘은 다음과 같다.

- 서명함수 $Sign()$: $Sign(x,c) \rightarrow (r,s)$ 여기서 임의 정수 $k \in Z_q$를 선정하고. $r = g^k \bmod q$, $h = H(c \parallel r)$, $s = hx + k \bmod q$ 를 계산한다.
- 검증함수 $Veri()$: $Veri(y,c,s,r) \rightarrow 0/1$ 여기서 g^s는 $y^h r \bmod q$와 일치 여부로 검증한다.
  - $g^{hx+k} = (g^x)^h g^k = y^h r \bmod q = g^s$

(3) 협동장치 서명조각 생성 및 사용자 서명합성 절차

Schnorr 임계 서명방식을 사용하기 전 사용자 등록 단계에서 사용자의 개인키 $sk \in Z_q$를 $(sk_i, i \in U_c)$ 조각으로 분해하여 sk_i를 협동장치 p_i 집합 U_c로 분배한다.

각 협동장치 $p_i, i \in U_c$이고, 여기서 U_c는 특정 사용자 협동장치 집합이다. 협동장치는 사용자와 통신이 가능



(Figure 4) 협동인증 절차

해야 하고 통신채널은 안전하다고 가정한다.

다음은 협동서명 방식 프로토콜이다,

① 협동장치 p_i는 임의 정수 $k_i \in Z_q$를 선정하고 $r_i = g^{k_i} \bmod q$을 계산 후 사용자에게 전송한다.

② 사용자는 모든 협동장치의 $(r_i, i \in U_c)$를 전송받아서 $r = \prod_{i \in U_c} r_i$을 계산하고, $h = H(c \parallel r)$ 계산 후 협동장치 p_i로 h를 전송한다.

③ 협동장치 p_i는 $s_i = h \bullet sk_i + k_i \bmod q$을 다시 계산하고 사용자에게 s_i를 전송한다.

④ 사용자는 Lagrange 계수 $\omega_i = \prod_{\substack{j \in U_c \\ j \neq i}} \frac{j}{j-i}$를 사용하여 $s = \sum_{i \in U_c} s_i \omega_i$ 계산한다.

⑤ 합성된 서명 (r,s)를 검색 웹이나 트래커에게 인증 정보로 보낸다.

⑥ 검색 웹과 트래커는 그 합성 서명을 사용자 공개키로 $Veri(y,c,s,r)$ 사용하여 검증한다

(4) 협동인증 절차 시나리오

협동인증이 필요한 시나리오는 기술영업을 위해서 해외로 노트북을 들고 가는 직원의 케이스이다. 보통 해외로 가는 직원은 아마도 태블릿, 스마트폰, 노트북 그리고 스마트워치 등을 가지고 갈 것이다.

해외 영업 출국 전 먼저 위 컴퓨팅 기능의 장비들을 등록한다. 이 노트북은 본 P2P 토렌트 분산 시스템의 사용자로 필요한 권한을 부여하고 등록한다. P2P 토렌트 시스템은 노트북에 검색 웹, 트래커의 공개키를 저장한다. 이 때 노트북은 협동인증을 위한 공개키와 개인키 쌍을 생성한다.

소유한 컴퓨팅 기능의 장치들 - 테블릿, 스마트폰, 스마트워치 등을 협동장치로 등록한다. 사용자 노트북은 생성한 개인키를 조각내서 각 협동장치에 전송한다.

사용자 노트북이 영업 과정에 비밀파일을 참조해야 할 경우 검색 웹을 통해서 사용자 인증을 할 때 검색 웹은 Challenge c를 사용자에게 보내고 다음의 협동인증을 수행한다.

① $k_i \in Z_q$, $r_i = g^{k_i} \bmod q$을 사용자 노트북에 전송

② 사용자는 $r = \prod_{i \in U_c} r_i$ $h = H(c \parallel r)$를 계산하고 각 협동장치에 전송

③ 각 협동장치는 $s_i = h \bullet sk_i + k_i \bmod q$를 계산하고 사용자에게 전송

④ 사용자는 $\omega_i = \prod_{\substack{j \in U_c \\ j \neq i}} \frac{j}{j-i}$, $s = \sum_{i \in U_c} s_i \omega_i$ 계산하고 $Sign(x,c) \rightarrow (r,s)$를 검색 웹에 전송

여기서 협동인증의 파라메터는 각 협동장치의 계산능력을 고려해서 적절한 값들을 사용해야 한다.

4. 보안성과 확장성 검증

본 논문은 기밀성과 인증성을 보완하고 토렌트 시스템의 피어 확장성을 활용하여 유출할 기기를 시스템에 동적으로 등록하여 외부 영업에서도 안전한 보안관리를 제공하는 P2P 분산 시스템을 제안하였다. 현재까지 임계 비밀조각 공유를 위해서 P2P 토렌트 분산 시스템에 적용한 연구는 매우 드물다. 일반적으로 P2P 토렌트 시스템은 단순한 구조 위에 파일 전송속도를 높일 목적으로 설계되었기 때문에 보안성을 위한 논의는 상대적으로 적었다 [18]. 그러나 본 시스템은 공개키로 교환되는 임시키 기반 암호화를 사용하고 다중 협동인증을 적용하여 토렌트 분산 시스템에 안전성을 강화하고 외부 유출 기기에도 보안성을 제공한다.

(1) (t,n)-임계 방식 보안성

여러 차례 언급한 것처럼 샤미르 비밀조각 (Shamir Secret Sharing) 임계 방식의 안전성은 널리 인정되고 있다. 임계 방식은 단 한 번의 접근으로 특정 자료를 얻을 수 없고, 임계 t개 조각을 얻어야 자료를 복원할 수 있다.

이러한 분산 보관 방식은 토렌트 P2P 시스템에서 사용되고 있고 그 파일의 전송속도가 빠르고 P2P 네트워크 구성이 단순한 여러 장점으로 비트코인 유통에도 채택되었다.

본 연구 시스템에서도 이러한 안정된 토렌트 P2P 시스템의 분산 피어에 비밀조각을 분산하여 일부 피어 공격으로 비밀자료 유출은 어렵다는 점을 감안하여 채택하였다. 그러나 토렌트 P2P 프로토콜은 자료 전송의 과정에서 기밀성, 무결성, 인증성을 보장하고 있지 않지만 본 연구는 이 안전성을 강화하였다.

(2) 노출 안전성

본 안전 비밀공유 시스템은 (t,n)-임계 방식으로 t개 비밀조각을 P2P 트래커가 임의 선정한 피어에만 분산하므로 비밀조각 피어 위치는 쉽게 알기 어려워 안전성이 높다. 비밀조각 피어 위치정보의 트래커 스웜프 L의 전송도 $E_k(L)$로 암호화 전송되므로 그 정보의 기밀성이 보장된다.

비밀조각의 전송은 트래커와 피어, 피어와 사용자 사이에서 발생하지만 모두 세션 동안 유효한 임시키를 사용하여 기밀성을 보장함으로 노출 위험에서 안전하다.

공격자가 임계 t개 비밀조각을 유출하는 것은 매우 어렵다. 이 공격은 먼저 P2P 내부망에 침투해야 하고 다시 t개 피어에 각각 침입해야 한다. 본 연구 시스템에서 피어 또는 트래커의 정보는 오직 임시키를 교환해야 하지만 이를 위해 트래커와 피어의 공개키를 얻어야 한다. 이것은 협동인증 과정을 거쳐야 하므로 공격자는 협동인증을 통과하기가 불가능하다.

(3) 사용자 협동 인증 안전성

본 연구 시스템의 사용자 인증은 다수 장치의 협동으로 인증서명을 생성하는 방식이다. 이는 사용자 단독으로 임의 서명을 생성할 수 없고 다중 협동장치가 실시간으로 생성한 서명 관련 조각을 모아서 사용자가 합성하여 서명을 생성하는 방식이다. 이는 외부에서 인증할 때조차 내부자 임의 서명이 불가능하고 등록된 협동장치의 실시간 서명조각으로만 가능함으로 인증 조작은 불가능하다.

협동장치의 임시 개인키와 같은 역할을 하는 임의 정수는 Fuzzy Extractor 방식으로 인체정보로 생성할 수 있기 때문에 협동장치 전부를 해킹하는 것은 불가능하다.

그 이유는 협동장치 p_i의 서명조각 s_i 계산에서 장치가 임의 정수 $k_i \in Z_p$로 $s_i \leftarrow h \bullet sk_i + k_i \bmod q$을 계산한다. 여기서 $k_i \in Z_p$는 각 장치 p_i의 고유한 생체기록 정보 b_i로 Fuzzy Extractor $k_i = Fuzzy(b_i)$로 생성할 수 있다. 그러나 본 연구에서는 Fuzzy Extractor는 구체적으로 다루지 않는다.

만일 일부 협동장치를 도난당하거나 잃어버릴 경우 노출될 계산된 정보는 $E_k(s_i)$, $E_k(sk_i)$, $E_k(h)$로 암호화 형태로 저장되므로 어떤 정보도 노출될 가능성이 없다.

만일 임시키의 노출로 해시값 h는 일방향성으로 알 수 있는 것이 없고 대수계산은 나머지 연산으로 소인수 분해의 어려운 문제로서 알아낼 것이 없다. 오직 서명조각 s_i는 노출될 수 있지만 인증서명마다 임의 정수 k_i로 계산되므로 s_i 일시적 실시간 값이다.

(4) 협동장치 서명조각 및 스웜프 재설정

사용자 협동인증에서 협동장치 p_i가 도난이나 분실되면 새로운 장치를 협동장치 U_c'에 등록하여 임계 t개 조각이 필요하고 사용자는 $sk \rightarrow (sk_j' \; j \in U_c')$로 개인키 조각을 다시 생성하여 분배한다. 많은 부담이 필요없는 계산이다.

사용자는 잃어버린 장치를 제외하고 협동인증에 참여할 장치의 수 $l(=|U_c|)$ 은 $t \le l$을 만족해야 한다. 사용자는 새 조각 $sk_j' \; j \in U_c'$를 장치 p_j', $j \in U_c'$에게 분배한다. 섹션 3.3의 협동장치 서명 생성과정을 다시 수행하여 $(s_j, p_j) \; j \in U_c'$를 생성한다.

스웜프를 생성하기 위해 각 장치는 임의 정수 pr_j을 Z_p에서 선정하여 개인키로, $pu_j = g^{pr_j} \bmod q$로 공개키 계산한다. 이 공개키를 트래커에게 전송하여 $(H(S), (s_j, p_j, pu_j) \; j \in U_c')$로 스웜프를 만들고 저장한다.

(5) 본 임계 방식의 효율성

본 연구가 제안한 비밀공유 시스템의 장점은 확장성과 효율성, 보안성 그리고 단순성이다.

첫째 확장성은 복잡한 운영으로 유지바용이 높은 중앙서버를 피하고 최근 선호하는 P2P 네트워크 분산 피어를 채택하므로서 본 안전 비밀공유 사스템의 구축비용이 저렴하고 그 확장성도 높다는 점이다. 그 확장성은 가격이 저렴한 피어를 추가하면 공유할 비밀의 규모에 관계없이 확장이 가능하다.

둘째 보안성은 임계 비밀조각 방식과 임계 협동인증의 다중인증 방식을 사용하므로 노출 확률이 낮아서 강력한 보안을 달성한다. 특히 임계 비밀조각 방식은 하나의 비밀에 집중될 수 있던 공격이 분산되므로 전체가 노출될 확률이 현격히 낮아진다.

임계 협동인증은 실시간 동적 인증이므로 협동장치 중 일부가 분실 또는 도난되어도 장치의 협동가능 시간이 동적으로 짧아서 그 가능시간이 지나면 새로운 장치를 재등록해야 하므로 이전 인증정보는 무의미하다. 따라서 협동인증은 장치 도용으로 인증을 Bypass 하는 것이 불가능하다.

셋째 단순한 프로토콜로 웹 기반 토렌트 P2P는 기능상 안정되고 효율적이다. 임계 비밀조각 방식도 Shamir 다항식 구성이 매우 쉬운 방식이므로 임계 방식의 계산부하는 매우 작다. 임계 인증 방식에서 Schnorr 방식도 임의 정수를 개인키로 하고 공개키는 생성자를 선정 정수로 지수승하는 계산으로 단순하다. 그럼에도 불구하고 다중장치의 서명 관련 조각 정보는 실시간 동적 계산에 기반하므로 매우 안전하다.

5. 결 론

본 안전 비밀공유 시스템에서 사용하는 암호기법은 Shamir와 Schnorr 방식이다. 좀 더 연구하고자 하는 분야는 타원곡선 암호방식을 적용한 협동인증 방식을 구현하는 것이다.

특히 ID 기반 암호기법을 사용하여 비밀조각 유통의 안전성을 Pairing 기반 방식을 적용하는 것이 매우 효율적일 것으로 보인다. 추후 연구는 이를 활용하는 방안을 제안하고자 한다.

오랜 연구였고 많은 논문을 접하면서 임계 방식의 장점을 많이 선호하게 되었다. 다음 연구에서 더 많은 것을 보여주려고 노력할 것이다.

참고문헌(Reference)

[1] BAE, KIM & LEE LLC, “The Report on Damage Examination of Korea Corporate Trade Secret.” Korean Intellectual Property Office, 2013. https://www.korea.kr/archive/expDocView.do?docId=35443

[2] Hyun-Jun Lee, Dae-Il Cho, Kab-Seung Kou, “A Study of Unidirectional Data Transmission System Security Model for Secure Data transmission in Separated Network,” Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, Vol. 5, No. 6, pp. 539-547, December 2015. http://dx.doi.org/10.14257/ AJMAHS.2015.12.12

[3] Financial Services Commission, “Comprehensive Measures for Security Enhancement of Banking IT system,” Policy Report, 2013. http://www.korea.kr/archive/expDocView.do?docId=34258

[4] Seung-gil Hong, Seung-chul Park, “A Design and Implementation of a P2P Streaming System with Considering Network Efficiency,” Journal of the Korea Institute Of Information and Communication Engineering (JKIICE) Vol. 17, No. 3, 2012. http://dx.doi.org/10.6109/jkiice.2013.17.3.567

[5] Jungeun Jee, Sangji Lee & 3, “A Logical Network Partition Scheme for Cyber Hacking and Terror Attacks,” KCC2011, Journal of KISS : Information networking, Vol. 39 No. 1, 2012. https://doi.org/10.13067/jkiecs.2013.8.9.1313

[6] Jin Li, Philip A. Chou and Cha Zhang, “Mutualcast: An Efficient Mechanism for Content Distribution in a Peer-to-Peer (P2P) Network,” 2005 IEEE International Conference on Multimedia and Expo, 2005. http:://www.cs.huji.ac.il, https://doi.org/10.1109/icme.2005.1521495

[7] Zeng Degui, Yishuang Geng, “Content Distribution Mechanism in Mobile P2P Network,” Journal of Networks, Vol. 9, No. 5, May 2014. https://doi.org/10.4304/jnw.9.5.1229-1236

[8] Kang Seung-Seok, “Content Distribution Mechanism in an All-Sender-All-Receiver Ad Hoc Network,” Proceeding of KFIS Autumn Conference 2005, Vol. 15, No 2, 2005.
https://www.koreascience.or.kr/article/CFKO200508824091845.jsp-k1ff8j=SSMHB4&py=2012&vnc=v27n6&sp=588

[9] Z. Xu; Y. Hu; L. Bhuyan, “Efficient server cooperation mechanism in content delivery network,” 2006 IEEE International Performance Computing and Communications Conference, Phoenix, AZ, USA, 10-12 April 2006. https://doi.org/10.1109/.2006.1629436

[10] Cristina Pérez-Solà, Jordi Herrera-Joancomartí, “The Bitcoin P2P Network,” March 2014, Conference: Proceedings of the 1st Workshop on Bitcoin Research (in Assocation with Financial Crypto 14),
https://10.1007/978-3-662-44774-1_7

[11] Sergey V. Bezzateev, D.Y.Kim, “COCkS’ 1[)’baSeo Scheme based Threshold Encryption Scheme,” 225, 2012. http://dx.d oorl d10.37451KIPSTC 2012.19 C.4.225

[12] Naoya Maki; Ryoichi Shinkuma, Tatsuya Mori, Noriaki Kamiyama, Ryoichi Kawahara, “A periodic combined-content distribution mechanism in peer-assisted content delivery networks,” 2013 Proceedings of ITU Kaleidoscope: Building Sustainable Communities, Kyoto, Japan, 22-24 April 2013,
https://doi.org/10.1109/icoin.2013.6496421

[13] NMC consulting group, “P2P Problem and Advent of P4P,” Netmanias Technical Documents,
https://www.netmanias.com/ko/post/techdocs Article No. 5201, network-protocol-p2p

[14] Aysajan Abidin, Abdelrahaman Aly, and Mustafa A. Mustafa, “Collaborative Authentication using Threshold Cryptography,” in Proc. of Emerging Technologies for Authorization and Authentication, pp. 122 – 137, 2019. https://doi.org/10.1007/978-3-030-39749-4_8

[15] Keju Meng, Yue Yu, Fuyou Miao, Wenchao Huang, Yan Xion, “Threshold Changeable Secret Sharing Scheme and Its Application to Group Authentication,” Information Processing Letters, Volume 157, May 2020.
https://doi.org/10.1016/j.ipl.2020.105928

[16] Alexandra Boldyreva, “Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme.” Y.G. Desmedt (Ed.): PKC 2003, LNCS 2567, pp. 31 – 46, 2003. cSpringer-Verlag Berlin Heidelberg 2003,
https://doi.org/10.1007/3-540-36288-6_3

[17] Victor Shoup, “Practical Threshold Signatures,” International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2000: Advances in Cryptology pp. 207-220, 2000.
https://doi.org/10.1007/3-540-45539-6_15

[18] H.J. Park, K.R. Park, “P2P Technology Trend and Application to Home Network,” Electronics and telecommunications trends, Vol. 21 no. 5, 2006.
https://doi.org/10.22648/ETRI.2006.J.210501

◐ 저 자 소 개 ◑

최 정 현(Cheong Hyeon Choi)
1984년 서울대학교 컴퓨터공학과(공학사)
1988년 조지아공과대학교 자연대학원 캄퓨터과학과(이학석사)
1992년 어번(Auburn)대학교 공과대학원 컴퓨터공학과(공학박사)
1994년～현재 광운대학교 경영정보학과 교수
관심분야 : 컴퓨터 네트워크, 정보보안, 암호학.
E-mail : chchoi@kw.ac.kr