http://dx.doi.org/10.14400/JDPM.2013.11.11.435

빅데이터 환경에서 미국 커버로스 인증 적용 정책

홍진근*
*백석대학교 정보통신학부

Kerberos Authentication Deployment Policy of US in Big data Environment

Jinkeun Hong*
Div. of Information and Communication, Baekseok University*

요 약 본 논문은 빅데이터 서비스를 위한 커버로스 보안 인증 방안과 정책에 대해 살펴보았다. 빅데이터 서비스 환경에서 하둡 기반의 보안기술에 대한 문제점에 대해 분석하였다. 또한 커버로스 보안 인증체계의 적용 문제를 고려할 때 미국의 상용 분야에서 발생하고 있는 주요 내용을 중심으로 적용 정책을 분석하였다. 커버로스 정책 적용과 관련하여, 미국은 크로스플랫폼 상호운용성 지원, 자동화된 커버로스 설정, 통합 이슈, OTP인증, 싱글사인온, ID 등 다양한 적용에 대한 연구가 이루어지고 있다.

주제어 : 보안정책, 빅데이터, Kerberos, 인증

Abstract This paper review about kerberos security authentication scheme and policy for big data service. It analyzed problem for security technology based on Hadoop framework in big data service environment. Also when it consider applying problem of kerberos security authentication system, it analyzed deployment policy in center of main contents, which is occurred in commercial business. About the related applied Kerberos policy in US, it is researched about application such as cross platform interoperability support, automated Kerberos set up, integration issue, OPT authentication, SSO, ID, and so on.

Key Words : Security Policy, Big data, Kerberos, Authentication

1. 서론

최근 빅데이터에 대한 관심이 증가함에 따라 보안에 대한 요구가 강화되고 있다. 이러한 요구는 빅데이터에 대한 통합분석의 요구, 수집과 성능 분석에서 병렬처리 적용, 잠재되어 있는 위협 탐지를 위한 사이버 상황인지 방안 도입, 실시간 분석 등을 특징으로 하는 통합보안 2.0 구조에 대한 강조로 나타나고 있다[1-2]. 빅데이터 보안은 하둡기반의 솔루션이 갖는 보안 이슈와 함께 커버로스인증에 대한 연구가 지속적으로 이루어지고 있다. A. Boldyreva와 V. Kumar는 커버로스에서 인증된 암호의 증명가능한 보안 분석 연구에서, 커버로스 5.0dp 대한 암호 분석을 심층적으로 하고 있다[3]. H.M.N. Al Hamadi 등은 모바일 에이전트 시스템(MAS)을 위한 분산 경량

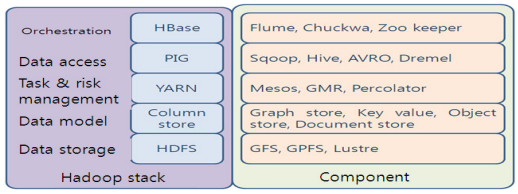
Received 18 October 2013, Revised 20 November 2013
Accepted 20 November 2013
Corresponding Author: Jinkeun Hong(Baekseok University)
Email: jkhong@bu.ac.kr

ISSN: 1738-1916

커버로스 프로토콜에 대해 연구에서, MAS를 위한 상호 인증과 키 분배 요구사항을 해결하는 방안을 제시하고 있다[4]. Inshil doh 등은 M2M 개방 IPTV 시스템을 위한 커버로스 기반의 개선된 보안 접근이라는 연구에서 수정된 커버로스 인증방안을 제시하고 인증에 소요되는 시간을 분석하고 있다[5]. Zhao Hu 등은 DH-DSA 키 교환을 기반으로 하는 개선된 커버로스 프로토콜에 대한 연구에서 DH-DSA 키 교환 최적화에 초점을 맞추고 있으며 유사 제안 모델과 보안측면(패스워드 추측공격, 재연공격, 중간자 공격, 알려진 키 공격, 비 forward 공격, 세션 상태 노출 공격)에서 비교 분석하고 있으며 커버로스 V5, PKINIT와 제안방안을 티켓 요구시간 측면에서 분석하고 있다[6]. Chundong Wan 등은 커버로스 인증 프로토콜의 프로세스를 분석하고, 기존 커버로스 인증프로토콜 제한점에 대해 분석하고 있다[7]. Woo Jeffrey 등은 그룹키 인증된 전달을 위한 커버로스 및 멀티미디어 인터넷 키 혼합방식에 대해 제시하며 보안 특성에 대해 분석하고 있다[8]. 또한 David Zage 등은 빅데이터를 사용한 공급체인 보안의 개선이라는 측면에서 직면한 제약요건이나 인식 및 계산측면에서 한계, 전략측면에서 trade off 라는 관점에서 접근하고 있다[9]. 연구된 대부분의 논문들은 빅데이터 서비스 환경에서 일어날 수 있는 보안 이슈 가운데 커버로스 인증이라는 측면에서 관심을 가지고 연구되어 왔다. 실제 커버로스 인증을 빅데이터 환경 즉 하둡 기반에 적용할 때 일어날 수 있는 문제점에 대해서는 아직 연구중에 있다. 본 논문은 빅데이터 서비스 환경에 커버로스 인증을 적용할 때 고려되고 있는 제반 이슈들과 그 적용 정책이라는 측면에서 분석하였다. 본 논문의 구성은 다음과 같다. 2장에서 빅데이터 하둡기반의 보안문제, 3장에서 미국 민간 빅데이터 환경에 적용되는 커버로스 인증 보안정책을 살펴보고 4장에서 결론을 맺었다.

2 빅데이터 환경에서 하둡기반 보안문제

하둡은 자바 기반의 MapReduce 개발 프레임워크(Pig-오픈 소스 언어이며 아파치 프로젝트, Hive-오픈 소스 언어이며 아파치 프로젝트로 하둡 환경에 SQL 인터페이스)이다. 역할 기반의 보안 관리를 필요로 한다(시스템 관리자, 데이터 관리자, 어플리케이션 관리자, 사용자). 대용량 처리 기반이 제공되나 장애, 파일 시스템 보안 측면에서 취약할 수 있다는 지적이 있으며, 보안을 포함한 기술지원 측면에서 어려움이 있을 수 있다는 점이 지적된다. 하둡의 구성은 HDFS - MapReduce(프레임워크) - Pig(언어, data flow), Hive(Batch SQL) 등 다양한 소스가 섞여 있으며, 현재 국가기관이나 사설 기업 내에서 하둡으로 구성하여 운영할 경우 가장 고려되는 사항 가운데 하나가 보안 부재라는 문제이다. 유닉스나 TCP/IP 같은 많은 오픈 소스처럼 하둡은 보안이 빌트인 되지 않은 분산 파일 시스템과 MapReduct 시설을 사용하는 아파치 서브 프로젝트로 알려진다. 하둡은 구글 MapReduce 프레임워크의 오픈 소스 버전에 소프트웨어 내에 보안이 설계되어 있지 않으며, 오픈 소스 하둡 커뮤니티의 경우 커버로스, 방화벽 사용, 기본 HDFS 퍼미션의 구현을 통해 몇 가지의 보안 특성을 지원하고 있다. 그런데 하둡 클러스터에서 커버로스는 필수 요구사항은 아니며 임의의 보안 적용 없이 전체 클러스터를 실행하도록 한다. 또한 커버로스는 클러스터 상에서 인스톨하고 설정하기가 어렵고, 액티브 디렉토리와 LDAP 서비스와 통합하기도 어렵고, 커버로스는 보안상에 적용하기에 어려움이 있어 하둡 사용자들에게 가장 기본적인 보안 기능을 적용하기에 제약이 있다는 점이 지적되고 있다.



[Fig.1] Security Architecture of Big data in Hadoop and NoSQL

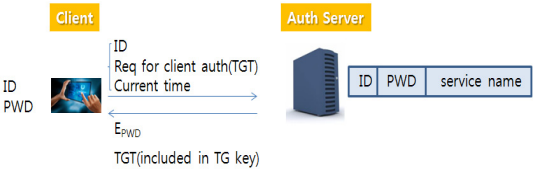
하둡 클러스터는 수십에서 수천의 노드로 구성되며, 분산 컴퓨팅 구조 특성은 분산컴퓨팅, 단편화된 데이터, 데이터 접근, 노드간 통신, 가상 비보안 등과 같은 문제에서 보안 고려사항이 제기되고 있다. 분산 컴퓨팅 문제에서, 데이터는 거대한 병렬 계산을 가능하고 임의의 리소스를 활용 가능하도록 처리되는데, 공격에 취약한 복잡한 환경을 만든다는 점이 지적된다. 중앙 집중화된 저장소는 보안상 안전하게 하기가 상대적으로 쉬우며 하둡과 빅데이터에 대한 보안 솔루션을 목적으로 가지고 빌드

시킬 때, 기관이나 기업의 데이터 센터와 하둡 클러스터 환경의 보안 요구사항을 만족시키는 분산 컴퓨팅 구조를 가지도록 설계할 것을 강조하고 있다. 데이터 단편화 문제와 관련하여, 빅데이터 클러스터 내의 데이터가 중복성 등을 보장하기 위해 다른 노드로부터(-로) 이동하는 다중 복사본과 함께 불안정하게 한다는 점이 이슈 되는데 데이터는 다중 서버를 통해 공유된 단편들로 분할될 수 있고 이 단편화가 보안측면에서 복잡성을 가중시킨다는 점이 지적된다. 데이터 접근 문제를 고려할 때, RBAC은 가장 중요한 DB 보안 프레임워크로 자리 잡고 있고 대부분의 빅데이터 환경은 스키마 레벨에서만 접근통제를 제공하고 역할과 관련된 접근에 의한 사용자들에게는 보다 구체성이 떨어진다는 점이 언급되고 있다. 노드간 통신에서는 하둡을 포함한 분산 처리에서 안전한 통신을 제공하지 않는데, TCP/IP 상에서 RPC를 사용할 뿐이라는 점이 지적된다. 가상으로 보안이 없다는 점은 빅데이터 스택이 거의 비보안으로 빌드한다는 점, YARN으로부터 웹 프록시 능력과 서비스 레벨 계정 부여를 제외하고, 데이터 저장이나 어플리케이션 또는 핵심 하둡 특성을 보호하기 위한 어떤 방법도 없다는 점이 한계점으로 언급된다. 모든 빅데이터 초기화는 웹 서비스 모델 상에서 빌드 되고, 공동의 웹 위협에 대응하는 어떤 방법이 없다. 빅데이터 통제와 관련된 데이터 보안과 프라이버시 문제에 대해 보안전문가들이 네트워크 에지에서 대부분 통제가 적용된다고 지적하며 공격자가 보안경계를 침투하게 되면, 빅데이터에 완전하고 무제한적으로 접근하게 되므로, 효과적인 방어선을 구축하기 위해 가능하면 데이터와 데이터 저장소에 근접하도록 통제를 위치시키라는 정책 수립을 제시하고 있다. 무엇보다 중요한 것은 데이터의 안전성인데 클러스터는 공격에 대응하여 높은 안전성을 가져야 한다. 즉 데이터 클러스터 자체 내에 임베디드 되는 빅데이터를 위한 클러스터 보안이 제공되어야 한다는 점이다. 가능하면 데이터에 근접하도록 보안을 하고, 방화벽과 같은 경계 보안 디바이스가 전달할 수 없는 보안을 제공하도록 설계해야 한다. 이 경우 데이터 센터 클러스터 내를 안전하게 보호함으로써, 보안경계가 침해를 입을 경우 클러스터와 민감한 데이터가 보안 wrapper에 의해 보호될 수 있도록 조치해야 한다. 그러므로 빅데이터 보안의 경우 오픈소스 환경에서 해결하기 어렵고 무시되는 빅데이터 관리(하둡 클러스터 환경 내의 정책, 컴플라이언스, 접근통제, 위험관리)의 보안 갭, RBAC 사용자 인증 강화, LDAP와 AD를 위한 지원을 포함하는 보안정책 프레임워크 내 하둡 클러스터의 통합을 단순화하는 작업, 로깅과 서치 및 감사 능력의 확장 등을 요구한다. 정리하면 RBAC 사용자 인증 프로세스에서 세분화된 접근통제, LDAP와 AD를 지원하는 보안 정책 프레임워크에 하둡 클러스터의 통합을 단순화시키는 것, 중앙집중화된 설정관리와 로깅 및 감사를 제공하여 리포팅과 포렌식에 대한 컴플라이언스 요구사항을 만족시킬 수 있도록 하둡 클러스터를 가능하게 하도록 설계하는 것이 요구된다. 하둡 구조에서 구조적인 보안 이슈는 분산노드, 공유데이터, 데이터 접근과 소유권, 노드간 통신, 클라이언트 상호작용, 비 보안에 대한 것이다. 빅 데이터의 분산 노드 문제에서, 이동하는 계산은 이동하는 데이터보다 비용이 저렴하며, 데이터는 리소스가 활용가능하고 거대하게 병렬 계산이 가능한 임의의 곳에서 처리됨에 따라, 공격이라는 복잡한 환경을 만들어 내고, 이는 이기종 플랫폼의 분산 클러스터를 통해 보안 일관성 유지를 검증하는 것이 어렵다는 점과 관련된다.

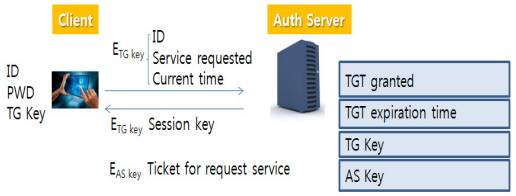
3 빅데이터 환경에서 커버로스 인증정책

3.1 커버로스 인증 개요

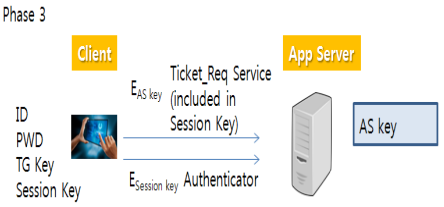
Fig.2는 커버로스 인증에서 티켓 부여 및 통신 서비스 절차를 나타낸 것이다.



(a) Phase 1 : initial step for ticket granting



(b) Phase 2 : Request for services from ticket granting



(c) Communication Service between Client and Application Service

[Fig. 2] Ticket Granting Service Procedure in Kerberos Authentication

빅데이터 서비스를 위한 하둡 기반에 적용되는 보안은 Hadoop1.0을 지원하면서 커버로스 인증과 RPC 다이제스트 방식 등이 제공되어 오고 있으나, HDFS에 적용되는 ACL이나 커버로스 인증이 보안요구기능을 만족시키기 어렵다는 지적인데, 네임 노드에서 클라이언트 미인증 또는 데이터 노드에 데이터 요청시 데이터 블록에 대한 권한 통제가 없다는 문제점이 지적되어 오고 있다. 자바 SASL (simple authentication and security layer)을 사용하는 RPC 인증의 경우 커버로스v5를 지원하는 GSSAPI, 다양한 하둡 토큰을 사용하는 인증에 요구되는 다이제스트 MD5를 적용하고, WebUI는 플러그인을 거쳐 인증을 수행한다. 커버로스는 사용자에게 한번 서명을 허용하는데, TGT를 획득한다. 여기에 신규 커버로스 티켓을 획득하기 위한 kinit를, 커버로스 티켓 리스트 klist, 커버로스 티켓 폐기 kdestroy를 사용하며 10시간동안 사용하되, 디폴트로 7일마다 갱신하는 정책을 수립한다.

3.2 미국 빅데이터 환경에 적용되는 커버로스 인증 보안 정책

크로스 플랫폼 환경에서 커버로스 상호운용성에 대한 연구에서 David는 윈도우즈 상호운용성을 위해 유닉스, 리눅스, Mac 통합 관점에서 접근하고 있다. 커버로스가 강한 인증을 제공하기 위해 크로스 플랫폼 상호운용성을 지원해야 하는 것과 자동화된 커버로스 설정(OpenSSH, Sambe, NFSv4; 아파치, J2EE 서버, SAP, Sybase, Oracle Advanced Security 등)를 통해 유닉스와 리눅스 서비스로 통합이라는 관점을 강조한다. OpenSSH는 DirectControl의 커버로스 라이브러리와 함께 링크되고 있으며, PuTTY는 윈도우즈 커버로스 라이브러리와 링크되고 있다. KDC 상호운용성 문제는 2 Way 크로스 신뢰를 통해 제공되는데 액티브 디렉토리 KDC는 보안 정책과 리소스 어카운트 관리에 사용되고 MIT KDC로부터 사용자는 허가된 액티브 디렉토리 단말과 어플리케이션에 로그인 할 수 있다[2]. Shumon Huque는 펜실베니아대학 커버로스 인증 정책에 대해 발표한 바 있다. 커버로스를 지원하기 위한 시스템은 RADIUS, 웹 싱글사인온, Federation (Shibboleth), 인증된 LDAP로 구성되며, 이 연구에서 웹 서비스를 위한 커버로스는 SPNEGO/HTTP Negotiate, KX.509와 IETF 표준의 폭넓은 지원과 채택으로 이루어지고 있음을 밝힌다. 또한 빅데이터 환경에서 보안 서비스를 지원하기 위해 HTTP용 Native Kerberos 지원과 무선 환경에서 EAP 인증방안, 네트워크 환경에서 IPSec지원, VoIP와 모바일 디바이스를 위한 커버로스, 다중 인증에 대한 다양한 보안 기술 적용에 대한 필요성을 강조하고 있다. 컬럼비아대학 Matt Selsky는 2010년 기준으로 콜럼비아대학 커버로스 인증을 위해 361K principal 사용과, 서비스 principal당 600 호스트를 지원하며, GSSAPI가 서버와 서버간에 인증과 암호를 위해 무겁게 사용되며, 1일당 2.4M AS_REQ와 1.8M TGS_REQ가 사용됨을 밝히고 있다. 코넬대학 Anderea Beesing가 코넬대학 교육환경에 적용되는 kerberos에 대한 연구에서는 커버로스 구현과 관련하여, NetIDs와 ServicesIDs를 사용하는 영역과 ApplicantIDs와 GuestIDs(legacy)영역으로 구분하여 적용하며, 두 개의 데이터 센터를 통한 중복성 문제, 2012년 하반기에 물리적인 박스로부터 VM으로 이동하고, 커버로스5 릴리즈 1.7, RHEL5 소프트웨어 버전으로 구축한다고 밝힌다. 통합지점(AuthN)에서는 웹 싱글사인온을 위한 CUWebLogin이 적용되고, 안전한 무선을 위한 Radius와 VPN이, WebDavauthN을 위한 역 프록시인 kProxy가, 그리고 연방 authN인 Shibboleth가 적용된다. NetIDs의 경우 생성/만료/패스워드 초기화를 위한 관리 도구에 사용하며, PeopleSoft 쿼리 기반의 신학생 NetID 생성을 위한 자동화된 메커니즘, 자가 서비스 활성화나 패스워드 변경과 초기화 용도, KBA 솔루션(RSA VerID) 용도로 사용된다. ServiceIDs는 서비스 제공자를 위한 자가 서비스 웹 어플리케이션에 사용되고, ApplicantIDs는 PeopleSoft 쿼리를 사용하는 자동화 메카니즘에, GuestIDs는 생성과 패스워드 관리를 위한 자가 서비스

어플리케이션에 사용된다. 그런데 인증을 적용할 경우 현실적으로 패스워드 기반의 인증이라는 싱글 factor 인증의 한계가 언급된다. 연방용 인증서 요구사항이나 인증할 수 있는 방안을 적용함으로써 오는 클라우드 환경에서 영향이라는 측면에서 여전히 숙제가 남아 있음을 언급한다.

Red Hat의 Dmitri Pal은 MIT 커버로스와 레드햇에서 자동화된 ID 선택이라는 측면에서 접근과 AuthHub를 주장한다. AuthHub는 외부 인증 방안에 대해 플러그 가능한 커버로스 KDC를 만드는데 OTP FAST를 기반으로 한다. 클라이언트와 외부 서버 사이에 KDC를 두고, KDC와 외부 서버는 플러그인되도록 하고, KDC와 클라이언트 사이에는 커버로스로 인증한다. 클라이언트는에는 SSSD(system security services daemon), PAM, KINIT를 그리고 클라이언트 커버로스 라이브러리에 플러그인을 둔다. 외부 인증을 지원하기 위한 KDC 개선에 초점을 맞추고 있으며, 퍼블릭 인터페이스를 사용한 프로토타입(Yubikey, 구글 authenti cator)을 구현한다. 이 연구에서는 향후 키 교환 기능, 자동화된 티켓 교환 서비스, GSSAPI 접속이 성립될 때 keytab에 접속을 차폐하기 위한 데몬설정, 단대단 스마트카드 지원 등에 대한 연구계획도 밝힌 바 있다.

Henry B. Hotz는 커버로스 인증서 발급 프로토콜 KX509에 대해 연구한 바 있는데, KX509는 X.509인증서를 얻기 위해 커버로스 티켓을 사용하기 위한 유선 프로토콜을 말한다. Pub/private 키를 생성하고 KCA와 함께 프로토콜 교환하고, 커버로스 신임장 캐시에 인증서를 저장하는 것과 관련되는 KX509, 커버로스 신임장 캐시에 저장되는 인증서 리스트와 관련된 KXlist, 신임장 캐시에 인증서와 키를 사용하는 PKI 지원을 구현하는 PKCS-11 라이브러리가 클라이언트에서 구현된다.

UDP 패킷을 통한 응답에서, 패킷에는 버전정보(2.0), 오류코드 없음을 나타내는 OK, 해시 응답필드(HMAC/SHA-1), 인증서(X.509), 오류 메시지가 포함된다. 그런데 Heny는 적용환경에 모든 커버로스와 X.509 고려사항이 적용되어야 하며, 커버로스와 PKI 정책과 관련 방안을 이해할 것(티켓과 인증서 생존시간, 공개적으로 인식된 KCA를 얻는 고민거리에 대한 감사)과 KX-509 인증서를 갖는 PKINIT를 하지 말라고 권고한다. 또한 모든 것이 평문이라는 점(해시가 모든 무결성을 보호해야 한다는 점, 프라이버시와 익명성이 지원되지 않는 점), 공개 키가 스니핑될 수 있고 재 사용될 수 있다는 점(요청자가 비밀 키의 정보를 증명할 수 없다는 점, 부인방지와 디지털 서명 어플리케이션이 깨질 수 있다는 점(키 사용 비트가 적용되지 않음), 인증서와 독립적으로 임의의 사용이 비밀 키 정보를 증명해야 한다는 점(TLS 클라이언트 OK)) 등 기본적인 제한 환경에 대해 지적한다. 추가적으로 SHA-1-HMAC 대신에 커버로스 체크섬을 사용할 것과 공개키 대신에 서명 요청된 PKCS-10(RFC-2986)을 보낼 것(요청에는 커버로스 ID가 묶여야 함), 그리고 e-text가 visibleString가 아닌 UTF8일 것을 강조한다. 이외에도 UDP 대신에 TCP를 사용할 것과 wait 라고 하는 새로운 메시지를 정의할 것과 새로운 종단 엔트리 인증서가 아닌 전체 인증서를 체인을 리턴할 것, 발행된 인증서를 위한 type 확장을 식별하는 것을 추가할 것을 주장한다. Linus Nordber는 MIT 커버로스를 위한 FAST (flexible authentication secure tunneling) OTP를 제안하고 있는데 이 방안은 사전인증 플러그인, OTP를 사용한 인증 사용자가 구현된 개념이다. OTP 모델은 이벤트 기반 모델(다음 OTP를 생성하기 위해 버튼을 누름)과 타임 기반 모델(생성된 다음 OPT와 어떤 것을 대기)을 소개하며, 챌린지를 추가하고, 생성된 OTP를 강화하고 토큰을 보호하기 위해 PIN이 사용된다. OTP 방안에서는 OATH(개방된 인증 개시), HOTP(OATH에 의한 HMAC 기반의 OPT), 비밀 값과 카운터 사용, 비밀 값과 카운터의 HMAC-SHA-1 계산, 결과를 정리하고 6개 이상의 십진수로 변환 처리, Oath 툴킷 패키지와 Yubikey 구현 등이 정의된다. 사전 인증은 4단계와 2단계가 있는데, 4pass는 클라이언트가 AS-REQ를 전송하고 KDC가 nonce와 함께 KRB-ERROR를 보낸다. 그리고 클라이언트는 암호화된 nonce와 함께 다른 AS-REQ를 보내고 마지막으로 KDC가 AS-REP를 전송한다. 2pass에서는 클라이언트가 암호화된 타임스탬프와 함께 AS-REQ를 보내고, KDC가 AS-REP를 전송한다. 반드시 nonce는 암호화해야 한다. 클라이언트와 KDC가 다음 OTP를 계산하고 공유된 비밀 값을 사용하여 키를 생성한다. 만일 nonce가 정상적으로 복호되며 클라이언트는 OTP 정보의 의해 클라이언트의 정보를 증명하고, KDC는 AS-REP를 암호화하기 위해 응답키를 사용하고, 키 정보에 의해 ID를 증명한다.

다른 대안으로 OTP가 KDC를 활용하지 않는 것으로, FAST 외장키가 클라이언트 키와 응답키로 사용되는 것이며, KDC의 어떤 인증도 제공되지 않는 것이다. OPT 플러그인 방식에서는 basicauth나 yubikey와 같은 opt 방안을 갖는 플러그인 시스템을 적용하고, OTP 토큰이 신규 key/valuetl_data type 메커니즘(set_string/ get_strings)로 principal을 위해 설정되고, 이때 principal은 설정된 0이상 토큰을 가지며, KDB에서 토큰은 ID, 메소드, 메소드로 통과된 선택된 분명하지 않는 것으로 구성된다. 인텔의 Ned Smith는 ID 보호기술에 대한 인텔의 모델을 제시한다. 인텔 ID 보호 기술 OTP를 웹 로그인에 적용하는 모델에서 제시된 절차는 다음과 같다. 먼저 사용자가 은행 로그인 페이지를 방문하고, 사용자는 UN과 PWD를 입력하며, 그때 True Cove가 발행된다. 이어 사용자가 마우스를 클릭하여 OTP PIN을 입력하고, PIN이 승인되면, OTP가 생성되고 채워져, UN과 PWD, OTP가 로그인을 위해 은행으로 전달된다.

또한 True Cove를 갖는 트랜잭션 보호절차에서는 먼저 클라이언트가 은행으로 인증하고 트랜잭션을 개시하면, 이어 은행이 클라이언트에게 웹 사이트가 암호화된 확인 스크린을 전송하게 된다. 이어 클라이언트에서 True Cove가 확인 스크린에 나타나 발급되고, 사용자는 PIN을 입력한다. 클라이언트가 은행으로 트랜잭션 확인이 리턴 되고 은행에서 PIN이 추출 검증되면 트랜잭션을 허가된다. 기업의 VPN 적용과 관련하여, 먼저 클라이언트 PIN을 요청할 수 있는 PEAT 키 쌍을 생성하는 셋업 어플리케이션을 실행하고, 클라이언트는 인증서를 등록하기 위해 PKI 서버로 접속한다. CA는 VPN 클라이언트와 적용을 위해 인증서를 발행한다. 다음 단계에서 셋업 어플리케이션은 한번 클릭으로 VPN 연결접속 클릭을 인스톨 하고, 클라이언트가 VPN 어플리케이션을 설치하고 자동으로 PEAT 인증서를 선택한다. 클라이언트는 TrueCove를 거쳐 PIN을 입력하여 진행한다. 인텔이 고려하는 클라우드 서비스 환경에서 로그인 유즈 케이스는 먼저 클라이언트가 인증서를 사용하여 사용자 인증을 요구하는 클라우드 서비스에 로그하면, 브라우저 쿠키가 클라이언트 인증서 능력을 식별하고 PEAT 키 인증서를 선택한다. 이어 클라이언트가 TrueCove PIN 패드를 사용하여 인텔 IPT로 인증하고, TLS VPN이 클라우드 어플리케이션 인터랙션에 의해 수립된다. 인텔에서 제시하는 PEAT 능력은 임베디드 암호 토큰(하드웨어 기반의 공개/개인 키 암호, 산업 표준 인터페이스 지원(CSP, KSP, PKCS11)), TrueCove를 거쳐 보호된 PINPAD(키 사용 권한, 클라이언트에 신뢰된 경로), 증명(신뢰 되는 하드웨어에 의해 보호된 키, 제로 터치 프로비저닝) 등이 특징이다. 인텔의 IPT 보안 모델은 Intel Core vProProcessor과 칩셋이 구동되는 견고한 환경에서 증명과 스마트카드 식별 능력을 가지며, ID 관리 제공자는 EPID 기반의 증명이 사용되는 신뢰 경계를 검증할 수 있다. 클라이언트 구조에서는 host(호스트 어플, 토큰 인터페이스), 칩셋 관리 엔진(TrueCove, PEAT, OTP, EPID, Sigma), Gfx 등이 있다. 인텔이 사용하는 자격증명서는 EPID(Enhanced Privacy Identifier), Sigma 프로비저닝 프로토콜, EAKE(EPID Key Ateestation Evidence)를 사용한다. 인텔은 추가된 강한 인증을 위해 OTP를 적용한 2 factor 인증을 적용하며, 다양한 환경에서 다양한 방법 즉 모바일 토큰(pledge), USB 키(Yubikey), SMS/ Email, 다양한 플랫폼(iPhone, BlackBerry, WinMobile 등) 상에서 이루어질 수 있도록 지원한다. 보다 안전한 인터넷 싱글사인온을 지원한다.

4. 결론

본 논문에서는 빅데이터 환경에서 적용되는 커버로스 인증 체계에 대한 적용 정책을 분석하였다. 빅데이터 서비스를 위해 적용되는 하둡 기반에서 일어나고 있는 보안 문제를 다루었으며, 특히 미국에서 현재 주요 쟁점으로 고려되고 있는 커버로스 인증체계의 적용 측면에서 분석하였다. 크로스플랫폼 상호운용성 지원, 자동화된 커버로스 설정에 대한 연구가 이루어지고 있으나, 여전히 통합 서비스, OTP 인증, 싱글사인온 적용, ID 등 다양한 적용에 관련된 지속적인 연구가 요청되고 있다. 본 논문의 분석 결과는 국내 빅데이터 서비스 환경에서 커버로스 인증체계의 현실적인 적용 측면에 기여할 것으로 판단된다.

REFERENCES

[1] SungHwan Kim, JungHo Eom, TaiMyoung Chung,

Big data Security Hardening Methodology using Attributes Relationship, ICISA2013, pp.1-2, 2013.

[2] Hojabri M., Rao K. V., Innovation in cloud computing: Implementation of kerberos version5in cloud computing in order to enhance the security issues, ICICES2013, pp.452-456, 2013.

[3] A. Boldyreva and V. Kumar, Provable-Security Analysis of Authentication Encryption in Kerberos, IEEE Security and Privacy 2007, pp.92-100, 2007.

[4] H.M.N Al-Hamadi, C. Y. Yeun, M.J. Zemerly, and M. Al Qutayri, Distributed Lightweight Kerberos Protocol for Mobile Agent System, IEEE GCC2011, pp.233-236, 2011.

[5] Inshil Doh, Kijoon Chae, Jiyoung Lim and Min Young Chung, An Improved Security Approach Based on Kerberos for M2M Open IPTV System, The 15th International Conference on NBiS2012, pp.754-759, 2012.

[6] Zhao Hu, Yuesheng Zhu and Limin Ma, An improved Kerberos protocol based on Diffie-Hellman-DSA Key exchange, 18th IEEE ICON2012, pp.400-404, 2012.

[7] Wang Chundong, Feng Chaoran, Security Analysis and Improvement for Kerberos Based on Dynamic Password and Diffie-Hellman Algorithm, EIDWT2013, pp.256-260, 2013.

[8] Woo J., Tripunitara M., Composing Kerberos and Multimedia Internet KEYing for Authenticated Transport of Group Keys, IEEE Trans. on Parallel and Distributed Systems, Vol.pp, Issue99, pp.1-11, 2013.

[9] David Zage, Kristin Glass, and Richard Colbaugh, Improving Supply Chain Security Using Big data, IEEE ISI2013, pp.254-259, 2013.

홍 진 근(HONG, JIN KEUN)

- 1991년 2월 : 경북대학교 전자공학과(공학사)
- 2000년 2월 : 경북대학교 전자공학과(공학박사)
- 2004년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

- 관심분야 : 정보보호정책, 통신네트워크보안
- E-Mail : jkhong@bu.ac.kr