암호컴포넌트 서비스 지원을 위한 HSSM 설계

박명찬*, 신동명**, 최용락*
*대전대학교 컴퓨터공학과
**한국정보보호진흥원
e-mail:mcpark@zeus.dju.ac.kr

Design of HSSM for Cryptographic Component Service Support

Myung-Chan Park*, Dong-Myung Shin**, Youg-Rak Choi*
*Dept of Computer Engineering, Daejeon University
**Korea Information Security Agency

요 약

기존의 보안 API는 각 사용자 요구사항 및 추진산업체 또는 표준단체, 개발환경 및 제공 서비스, 함수의 명칭, 자료구조 등이 독립적인 구조를 가지고 있어 각 보안 API에 대한 총괄적 표준화에 어려움이 있었다. 또한, 오늘날 하루가 다르게 급변하는 요구사항에 대하여 적시성을 제공하기에 부적합하였다. 이에 따라 소프트웨어의 품질을 보증하고 적시성을 제공할 수 있는 컴포넌트 기술이 제안되었다.

본 논문에서는 다양한 소프트웨어 비즈니스 모델 개발에 다목적으로 활용 가능한 새로운 패러다임의 컴포넌트 설계기법을 표준적 암호서비스 기술 개발에 도입하여 암호서비스에 대한 상호운용성의 확보와 이기종 시스템간의 상호호환성 및 필요한 모듈의 추가 및 변경의 용이성 등을 제공하기위하여 암호컴포넌트 서비스 지원을 위한 HSSM을 설계하였다.

1. 서론

정보통신기술의 발전과 더불어 보안 위협요소 역시 더욱 증가하였다. 이에 따라 보안 위협요소를 방어하기 위한 보안서비스 기능의 효과적 정합 방법에 대한 연구개발이 대단히 주요해졌다. 그러나, 각 응용 분야별 보안기술의 개발은 이기종간 호환성의 결여로 인한 중복된 투자손실 등의 문제점이 발생되었다. 이러한 문제점을 해결하기 위하여 범용적 사용이 가능한 표준의 개발이 지속적으로 요구되었고, 이를 위하여 보안 API(Application Program Interface)가 설계되었다[1].

기존의 보안 API는 각 사용자 요구사항, 추진 산업체 또는 표준단체, 개발환경 및 제공 서비스, 함수의 명칭 및 자료구조 등이 모두 차이가 있다. 그러므로 개별적으로 추진된 각 보안 API에 대하여 총괄적으로 표준화하는 것은 어려운 일이다. 또한 오늘날 하루가 다르게 급변하는 요구사항에 대하여 적시에 최적의 소프트웨어를 제공하기에 부적합하였다. 각 단체별 추진된 기존의 보안 API 기술표준에 대한 국내 적용은 다음과 같은 문제점을 갖고 있다.

먼저 국내의 알고리즘 표준이나 적용환경은 국제 보안 API 표준을 전혀 고려하고 있지 않다는 것이다. 둘째, 기존의 각 보안 API는 각 사용자 요구사항, 추진 산업체 또는 표준단체 등이 모두 상이하여 보안 API의 총괄적 표준화가 불가능하였다. 셋째, 특정한 보안 API의 선정시 항상 그 보안 API 모델에 종속적일 수밖에 없으므로 국내 실정에 맞는 독자적인 표준개발이 필요하게 되었다. 넷째, 기술적인 난이도가 날로 증가하고 있으며, 이러한 기술들의 연구 개발과 표준화를 분리하여 수행하는 것이 사실상 불가능해지고 있다는 것이다[1,2,3].

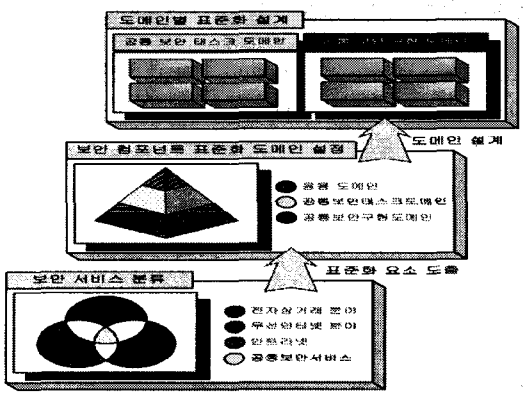
따라서, 다양한 소프트웨어 비즈니스 모델 개발에 공통적으로 활용될 수 있는 새로운 패러다임의 컴포넌트 설계기법을 표준적 보안서비스 기술 개발에 도입하고, 표준화된 컴포넌트를 소프트웨어 시스템에 Plug &Play 방식으로 조립함으로써 개발공정의 적시성과 생산성을 향상시킬 필요가 있다[4,5].

본 논문에서는 암호컴포넌트 인터페이스 표준화를

위하여 암호컴포넌트 설계에 있어 기반이 되는 상위 레벨 보안서비스 관리[HSSM: High-level Security Service Management]모듈을 설계하여 다양한 응용 레벨에서의 상호호환성을 제공하고자 한다.

2. 암호컴포넌트 개념 설계

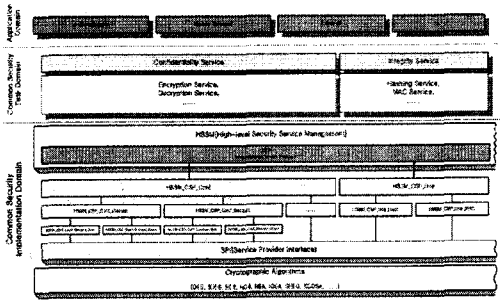
범용 암호컴포넌트 인터페이스 표준화를 위한 단계적인 접근을 위하여 크게 3단계로 분류하였다. 각 단계는 보안서비스 분류, 보안컴포넌트 표준화 도메인 설정, 도메인별 표준화 설계 단계로 그림 2와 같이 분류하였다.



(그림 2) 암호컴포넌트 개념 설계

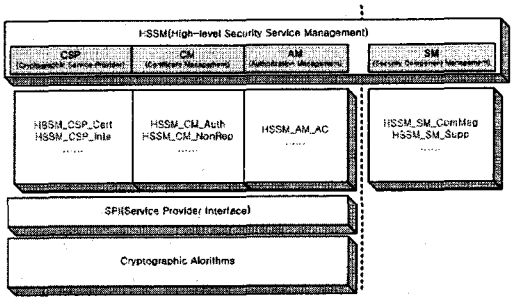
첫 번째 단계는 현재 응용 소프트웨어에서의 보안서비스의 분류 단계로 일반적 인터넷 환경에서의 쇼핑몰, 홈뱅킹 등의 전자 상거래 분야 그리고 유선과 더불어 부각되고 있는 차세대 무선 인터넷 분야, 기업 및 학교, 정부 등에 사용하는 인트라넷 등으로 분류할 수 있으며, 이러한 서비스에 대하여 공통적으로 재사용 가능한 보안서비스인 무결성, 기밀성, 인증, 접근통제 서비스를 도출한다.

두 번째 단계는 분류된 공통 보안서비스를 중요요소로 표준화 도메인을 그림 3과 같이 크게 응용 도메인, 공통 보안 태스크 도메인, 공통 보안 구현 도메인으로 분류한다. 먼저 응용 도메인은 일반적 응용 소프트웨어나 클라이언트가 올 수 있다. 예로, 전자상거래 분야, 무선 인터넷 분야, 인트라넷 등의 응용프로그램이 존재한다. 두 번째 공통 보안 태스크 도메인은 공통 보안서비스를 응용 프로그램 등의 클라이언트에 제공한다. 공통 보안 태스크 도메인은 서비스 제공에 있어 암호학을 아는 사람에서, 암호학을 모르는 클라이언트 모두에게 공통 보안서비스를 제공한다. 마지막 공통 보안 구현 도메인은 공통 보안 태스크 도메인을 실질적으로 구성하는 보안서비스 인터페이스를 제공한다. 즉, 상위의 공통 보안 서비스에서 하위의 암호화 알고리즘이나, 키 생성 함수 등의 함수들을 포함한다.



(그림 3) 암호컴포넌트 도메인 분류

세 번째 단계는 분류된 공통 보안 태스크 도메인과 공통 보안 구현 도메인에 대하여 단계별로 설계한다. 본 논문에서는 그림 4에서의 공통 보안 구현 도메인에서 각 상위 도메인으로 공통 보안서비스를 지원하는 HSSM(High-level Security Service Management)를 설계하여 실제적인 보안서비스 연결 및 접속관리 등의 서비스를 제공하고자 한다.



(그림 4) 공통 보안 구현 도메인 구성도

3. HSSM

3.1 HSSM 구조

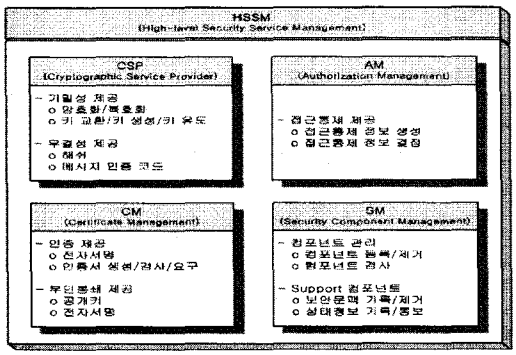
HSSM(High-level Security Service Management)은 상위계층과 하위계층간의 암호서비스를 위한 상호동작성 관리 기능 및 암호컴포넌트의 등록 및 해제, 컴포넌트 유효성 검증, 사용 중인 컴포넌트의 상태 정보관리, 다중 암호서비스 제공을 위한 연결 관리의 역할을 수행한다. 그림 5는 HSSM의 구성도를 보여준다. HSSM는 크게 4가지로 구성되며 각 기능을 요약하면 다음과 같다.

1) CSP: CSP(Cryptographic Service Provider)는 공통 보안서비스 중 무결성과 기밀성 서비스를 지원한다. 즉, 기밀성을 위한 암호화/복호화, 키 관리 등의 인터페이스를 제공한다.

2) CM: CM(Certificate Management)는 인증 및 부인봉쇄 서비스를 지원을 위하여 전자서명, 인증서 관리 등을 제공한다.

3) AM: AM(Authorization Management)는 접근통제 서비스의 지원을 위하여 접근통제 정보 정의 및 생성, 통제 기능을 제공한다.

4) SM: SM(Security Component Management)는 HSSM의 구성요소 및 하위 컴포넌트 간의 상호동작성을 보장하기 위하여 각 컴포넌트에 대한 관리 및 기타 Support 기능을 제공한다.

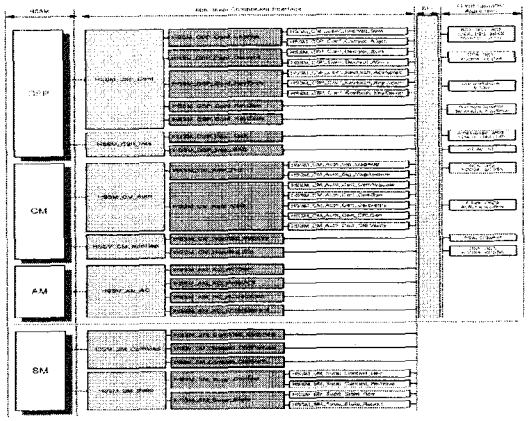


(그림 4) HSSM 구성도

3.2 HSSM 설계

그림 6은 상위 컴포넌트와 하위 컴포넌트 연결을 지원하는 HSSM의 기능에 대한 인터페이스로 CSP, CM, AM, SM등을 지원하는 컴포넌트로 구성된다. 즉, 실질적인 HSSM의 구성요소에 대한 인터페이스 및 컴포넌트 연결 및 해제 기능을 제공한다. 또한, 사용자 레벨에 따른 다양한 수준의 암호서비스를 지원한다.

HSSM 지원을 위한 암호서비스별 인터페이스 설계를 위하여 해당 인터페이스는 크게 3단계의 약한, 보통, 강한 수준의 보안서비스를 제공한다. 약한 수준은 보안 지식이 없는 클라이언트로 상위 수준의 보안서비스를 제공하고, 보통 수준은 일반적인 보안 지식을 알고 있는 사용자로 약한 수준을 포함한다. 강한 수준은 높은 보안 지식을 알고 있는 사용자로 약한, 보통 수준의 기능을 모두 사용가능하다. 보안 서비스별 인터페이스는 다음과 같다.



(그림 5) 상위 컴포넌트 인터페이스 설계

1) 기밀성 서비스 인터페이스

기밀성 서비스의 제공을 위하여 암호화/복호화, 키 교환/생성/유도등의 인터페이스로 구성된다. 약한 수준은 클라이언트가 보안 지식이 없을 때 이용 가능한 인터페이스로 상위 수준의 보안서비스를 요청한다. 즉, 추가적인 선택 없이 기본 인터페이스만을 제공한다. 보통 수준은 클라이언트가 일반적인 보안 지식을 알고 있을 경우 이용 가능하며 기밀성을 위한 암호화/복호화 및 키 교환/생성/유도 등을 직접 선택할 수 있는 인터페이스를 제공한다. 강한 수준은 클라이언트가 높은 수준의 보안 지식을 알고 있을 경우 이용 가능하며 기밀성을 위한 최하위 암호 알고리즘을 선택하여 적용 할 수 있다. 또한, 약한, 보통 수준의 기능을 포함한다.

2) 무결성서비스 인터페이스

무결성 서비스의 제공을 위하여 해쉬 및 메시지 인증 코드 등의 인터페이스로 구성된다. 약한 수준은 클라이언트가 보안 지식이 없을 때 이용 가능한 인터페이스로 상위 수준의 보안서비스를 요청한다. 즉, 추가적인 선택 없이 기본 인터페이스만을 제공한다. 보통 수준은 클라이언트가 일반적인 보안 지식을 알고 있을 경우 이용 가능하며 무결성을 위한 해쉬 함수 또는 메시지 인증 코드 중 선택적으로 적용할 수 있는 인터페이스를 제공한다. 강한 수준은 클라이언트가 높은 수준의 보안 지식을 알고 있을 경우 이용 가능하며 기밀성을 위한 최하위 암호 알고리즘을 선택하여 적용 할 수 있다. 또한, 약한, 보통 수준의 기능을 포함한다.

3) 인증서비스 인터페이스

인증 서비스의 제공을 위하여 전자서명 및 인증서

관리 등의 인터페이스로 구성된다. 약한 수준은 클라이언트가 보안 지식이 없을 때 이용 가능한 인터페이스로 상위 수준의 보안서비스를 요청한다. 즉, 추가적인 선택 없이 기본 인터페이스만을 제공한다. 보통 수준은 클라이언트가 일반적인 보안 지식을 알고 있을 경우 이용 가능하며 인증을 위하여 전자서명 및 인증서 등을 선택 적용할 수 있는 인터페이스를 제공한다. 강한 수준은 클라이언트가 높은 수준의 보안 지식을 알고 있을 경우 이용 가능하며 기밀성을 위한 최하위 암호 알고리즘을 선택하여 적용할 수 있다. 또한, 약한, 보통 수준의 기능을 포함한다.

4) 부인봉쇄 인터페이스

부인봉쇄 서비스의 제공을 위하여 공개키 방식과 전자서명을 이용한 방식 등의 인터페이스로 구성된다. 약한 수준은 클라이언트가 보안 지식이 없을 때 이용 가능한 인터페이스로 상위 수준의 보안서비스를 요청한다. 즉, 추가적인 선택 없이 기본 인터페이스만을 제공한다. 보통 수준은 클라이언트가 일반적인 보안 지식을 알고 있을 경우 이용 가능하며 부인봉쇄를 위하여 공개키를 이용한 방식과 전자서명을 이용한 방식 등을 선택할 수 있는 인터페이스를 제공한다. 강한 수준은 클라이언트가 높은 수준의 보안 지식을 알고 있을 경우 이용 가능하며 기밀성을 위한 최하위 암호 알고리즘을 선택하여 적용 할 수 있다. 또한, 약한, 보통 수준의 기능을 포함한다.

5) 접근통제 인터페이스

접근통제 서비스의 제공을 위하여 접근통제 정보의 생성 및 결정 등의 인터페이스로 구성된다. 약한 수준은 클라이언트가 보안 지식이 없을 때 이용 가능한 인터페이스로 상위 수준의 보안서비스를 요청한다. 즉, 추가적인 선택 없이 기본 인터페이스만을 제공한다. 보통 수준은 클라이언트가 일반적인 보안 지식을 알고 있을 경우 이용 가능하며 접근통제를 위한 접근통제 정보 생성 및 결정 그리고 적용 등을 선택할 수 있는 인터페이스를 제공한다.

6) 컴포넌트 관리 인터페이스

컴포넌트 관리를 위하여 컴포넌트 등록 및 컴포넌트 제거, 검증 등의 인터페이스를 제공한다. 컴포넌트 관리 인터페이스는 각 컴포넌트에 대한 등록 및 제거, 검증 등의 인터페이스를 제공한다.

7) Support 컴포넌트 인터페이스

Support 컴포넌트 인터페이스는 각 컴포넌트에 대한 상태 정보 저장 및 통보 기능을 수행한다. 즉, 각 서비스에 대한 보안문맥 관리 등의 기능을 제공한다. 이를 위하여 보안문맥 관리 및 상태 관리 인터페이스를 제공한다. Support 컴포넌트 인터페이스의 주요 함수는 보안문맥 관리 기능과 상태정보 관리 기능으로 정의할 수 있다. 먼저 보안문맥 관리 함수에서는 각 컴포넌트에 대한 보안문맥 저장 및 제거 기능을 수행하고, 상태 관리 함수에서는 각 컴포넌트의 상태정보에 대한 저장 및 통보 기능을 수행한다.

4. 결론

인터넷의 보급과 IT 기술의 발전으로 개발자 중심의 S/W 개발 방식에서 사용자 중심의 개발환경으로 변화되는 시점에서 기존 보안서비스에 대한 한계 및 문제점을 분석하고, 빠르게 바뀌어 가는 환경으로부터 적절하게 대응할 수 있는 컴포넌트 기반의 암호컴포넌트 표준화를 위한 3단계 설계방안을 제안하였다.

본 논문에서는 범용적 암호컴포넌트의 서비스 지원을 위한 핵심 기술인 공통 보안 태스크 단계에서의 HSSM의 기능을 정의하고 각 기능을 설계하였다. 설계된 HSSM은 향후 암호컴포넌트의 핵심 기술로 재사용성의 극대화, 생산성 증가 및 상호운용성의 확보와 이기종 시스템간의 상호호환성 등을 제공한다. 향후, 본 논문의 결과를 활용하여 개발공정의 적시성 및 생산성을 향상시킬 수 있는 다목적 암호컴포넌트 기술의 기반이 될 것으로 기대된다.

참고문헌

[1] 최용락 외6인, "보안 API 표준화 연구", 한국정보보호센터, 2000.12.

[2] 박명찬, 신동명, 최용락, "다목적 암호컴포넌트 서비스 요구사항 분석", 한국인터넷정보학회 제3권 2호, 2002. 11.

[3] 박영신, 신동명, 최용락, "보안서비스를 위한 컴포넌트 설계표준 기술 분석", 한국정보보호학회 충청지부, 2002. 7.

[4] 조남규, "분산 컴퓨팅 패러다임을 위한 컴포넌트 기술에서 CBD로의 움직임", COOL Software, 2000. 6.

[5] 배두환, "컴포넌트 기술발전 동향과 전망", 소프트웨어 컴포넌트 ,창간호 특집, 2002. 7.