

유니버설미들웨어기반 생명주기 보안에너지 서비스플랫폼 연구

이해준¹ · 황치곤¹ · 윤창표^{2*}

The Security Life Cyler Energy Service Platform for Universal Middleware

Hae-Jun Lee¹ · Chi-Gon Hwang¹ · Chang-Pyo Yoon^{2*}

¹Department of Convergence Software, Kyungmin University, Uijeonbu-si 11618, Korea

^{2*}Computer&Mobile Convergence, GyeongGi College of Science and Technology, Siheung-si 15073, Korea

요 약

전력서비스를 지원하는 융합보안시스템 단말장치는 상대적으로 고도의 신뢰성이 요구된다. 특히, 에너지서비스의 복합적인 통신과 데이터 인터페이스장치간의 보안시스템이 유기적으로 연동되어야 한다. 기존의 서비스와 연관성을 두어 시스템을 구축하기 위해서는 시스템독립성과 확장성을 지원하는 생명주기 방식의 보안 서비스플랫폼이 요구된다. 생명주기를 지원하는 유니버설미들웨어방식의 Security Layer를 활용하는 것이다. 이 융합보안 플랫폼은 첫째, 실시간으로 운영되는 통신과 데이터 및 응용서비스에 대해 독립적으로 동작 가능하도록 서비스 단위로 모듈화하였다. 둘째, 보안 레이어 개념을 적용하여 외부 보안 서비스에 대하여 보안모듈의 설치, 삭제, 시작, 중지 및 갱신을 통해 생명주기 모듈로 배포하는 플랫폼 모델을 구성하고 평가하였다. 그리하여, 실시간으로 운용되는 프로토콜의 실행상태에서 프로토콜 전송 서비스의 안정성과 하드웨어시스템에 독립적인 모듈단위의 보안서비스를 지원하도록 하였다.

ABSTRACT

Security services that support electric energy service gateway require relatively high reliability. In particular, the application services that accompany communications and data are run organically. Each of the security services should support a secure service platform that supports a secure, scalable life cycle for existing services which should be extends security layer of Universal Middleware. In this convergence platform, it is the study of security transfer modular services that allow independent life cycle management of systems through Universal middleware. First, It is modular in terms of energy consumption service and data, enabling real-time operation, communications, remote management and applications. Second, the life cycle of the secure module to support start, stop and updating of the security module by applying the security policy module layer concept. It is modular system enabling to design of dyanmic models in the smart grid, the service was intended to be standardized and applied to the security service platform.

키워드 : 유니버설미들웨어, 보안플랫폼, 차세대에너지 보안, 보안미들웨어

Key word : Universal Middleware, Security Platform, Next Generation Energy Security, Security Middleware

Received 24 May 2017, Revised 25 May 2017, Accepted 01 June 2017

* **Corresponding Author** Chang-Pyo Yoon(E-mail:cpyoon@gtec.ac.kr, Tel:+82-31-496-6410)

Computer&Mobile Convergence, GyeongGi College of Science and Technology, Siheung-si 15073, Korea

Open Access <https://doi.org/10.6109/jkiice.2017.21.6.1197>

print ISSN: 2234-4772 online ISSN: 2288-4165

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright © The Korea Institute of Information and Communication Engineering.

I. 서 론

최근 융합단말 시스템의 특징은 제조사의 기능적 요소, 서비스사용, 배포정책이 복합적으로 내포되어있다. 이러한 복합적 요소에 필요한 보안과 인증은 효율성과 고도의 신뢰성이 조화를 이루어야 한다.

유니버설미들웨어와 생명주기 방식은 융합보안 시스템을 구성하는데 있어 다양하고 복잡한 에너지공급자와 제조사 기기의 지능화, 유지보수, 원격 관리서비스를 비롯한 지속적인 요구사항을 실시간으로 지원한다. 이렇게 구성된 플랫폼으로 보안시스템을 배포, 공급, 관리하게 되면 변동성이 높은 시스템을 운용하는데 소요되는 불필요한 시간과 비용을 절약할 수 있다.

유니버설미들웨어기반의 융합보안 시스템에 필요한 유무선 융합방식을 적용할 수 있는 분야로는 스마트홈과 자동차분야의 수요공급 모델이 대상이 될 수 있다. 이 모델은 공급자 중심의 보안 서비스보다는 사용자 중심의 서비스 모델을 적용하고 있으며 편의성보다는 공급망의 안정성을 우선으로 한다.

유니버설미들웨어의 유무선 융합을 지원하는 프로토콜로는 TR-069¹⁾, OMA²⁾, JTC1³⁾, HGI를 비롯하여 지속적으로 추가되고 있다. 이 때문에 휴대폰, 웹, SNS를 비롯하여 대체 가능한 유무선 융합 에너지 단말시스템에 적용이 가능하다.

시스템상의 Life Cyler Security Platform(이하 LCSP)의 기술적 모티브는 전력계통 서비스망에서의[1] 데이터전송 표준화, 융합서비스의 통신 표준화에 각각 초점에 두고 있다. 그림 1에서는 LCSP단말이 스마트그리드[2]보안모듈로써 유니버설미들웨어에서 Security Layer로 동작하는 것을 나타내고 있다.

Security Layer는[3] 독립적이면서 분류가 가능한 OSGi⁴⁾ 형태로[4] Inventory구조이고, LCSP API상에서 인터페이스로 동작하는 Open Radius : Remote Authentication Dial-In User Service, 요청시스템과 서비스 액세스 권한을 부여하기 위해 서버와 통신하는 클라이언트/서버 프로토콜모듈 서비스를 적용하였다.

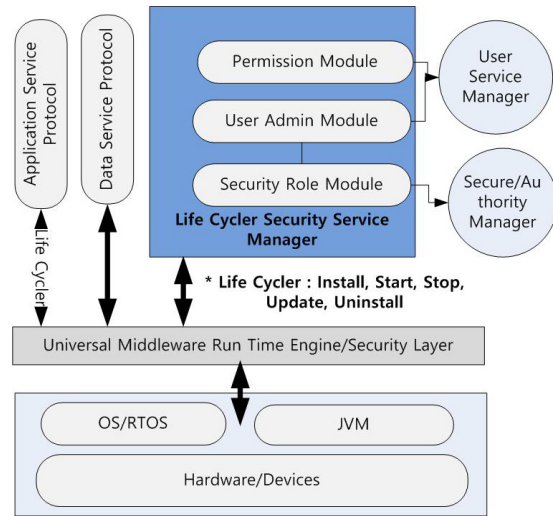


Fig. 1 Architecture of LCSP Security Module.

II. 본 론

2.1. 유니버설 보안 모듈의 구성

보안정책의 핵심 모듈은 공급사와 수요자간의 서비스표준화 모듈과 통신시스템 표준화 모듈이다. 이 모듈들이 유기적인 생명주기 시나리오를 찾아 모듈화 하는 것이다. 통신서비스와 에너지 수요연계를 위한 제조사 측의 보안 서비스를 제공한다.

에너지 수요관리 시스템에서 필요한 확장분야로는 IoT, BigData, Cloud 컴퓨팅에서[5] 생명주기로 동작하는 보안 서비스 모듈로 제공될 수 있다.

각 서비스 모듈이 보안시스템에 독립적으로 설계할 수 있다. 이 모듈은 다음과 같이 정리할 수 있다.

- 원격관리와 원격진단에 적용하는 보안모듈의 표준화 모듈
- 보안 레이어 모듈과 이기종 분야의 사용자와 관리자 간의 연계한 표준화 모듈
- 서비스 제어와 서비스 관리에 적용하는 보안 서비스 표준화 모듈

1) TR-069 : Technical Report 069 의 약자, DSL포럼(Broadband포럼), CWMP 기술 명세서
 2) OMA : Open Mobile Alliance, 휴대폰 표준 프로토콜 제정 단체 및 규격
 3) JTC1 : ISO/IEC 융합표준 프로토콜 단체 및 규격
 4) OSGi : Open Services Gateway initiative, 유니버설미들웨어를 적용한 민간표준 단체 및 규격

융합 서비스모듈의 보안정책은 스마트그리드 보안 시스템에 적용하기 위해 응용 라이브러리와 데이터 및 통신모듈에 녹아 들어 지원한다. 이 모듈의 구체적인 항목은 다음과 같다.

- 전력 서비스단말의 독립적인 Security Layer 서비스 모듈
- 전력 서비스단말의 Data, Protocol, Interface 확장 모듈

2.2. LCSP 융합보안 단말시스템

스마트그리드의 통신단말상에서 보안시스템을 구성하는 표준화 모듈이다. 실시간 운영체제에서 에너지서비스의 공급과 제어에 따른 수요공급변화 데이터를(6) 실시간으로 처리하는 보안시스템으로 다음과 같은 서비스를 지원한다.

- Security Signal Service
- Dynamic Control Service
- Data Parameter Service

보안 서비스 적용방법으로는 유니버설미들웨어를 사용하여 하드웨어 기능에 독립적인 Dynamic Security 모듈을(7) 지원한다. 이 모듈은 시스템 실행영역에서 응용서비스와의 독립성, 확장성, 이식성을 보장한다. 가상머신상(8) 보안서비스의 적용으로 보안프로토콜로 모듈로 구성한 것이다.

그림 2는 융합보안 서비스단말의 시스템 구조와 모듈의 개념을 나타내고 있다. 개념적으로 보면 응용서비스인 전력서비스와 융합단말에 탑재되는 전력기기, 전력통신 프로토콜인 DNP(6) 프로토콜과 ICBMS(7)에 반영하여 Dynamic Service 모듈로 구성하였다(8,9).

이 서비스들은 인증 클라이언트와 인증 서버모듈과 유기적인 생명주기로 모듈간의 시나리오를 연동하여 구성한다. 인터페이스 모듈을 통해 LCSP 상의 생명주기관리가 가능한 형태로써 최종 응용서비스 구동에 필요한 시스템 패키지과 인접한 보안 노드인 $|N| \times$

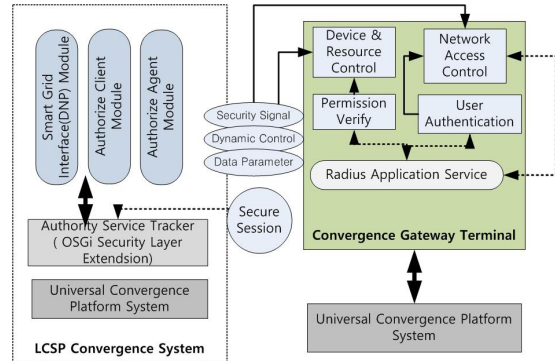


Fig. 2 LCSP System Architecture

$|N+1| \times |N+2|$ 를 최대 $|S|^9 + |S+1| + |D|^{10} + \alpha^{11}$ 로 효율화 하여 S노드의 보안 시스템 자원을 유지한다.

2.3. LCSP 에너지 보안 시나리오 서비스 모델

보안 시나리오를 구성하기 위한 에너지 서비스 모델을 설계할 때는 서비스를 공급하는 공급자 측면의 요구 사항과 이를 소비하는 에너지 검침장치간의 시나리오 모델로 설계할 수 있다. 이 과정에서 LCSP 시스템으로 설계할 수 있는 보안 표준 모듈은 다음과 같다.

- Connection Security Module
- Data Security Module
- Application Security Module
- Authorize Protocol Security Module

이렇게 보면 Security Module를 별도의 Security Layer Module로 생명주기를 지원하는 실행시스템으로 시스템을 적용할 수 있다. 따라서, Connection, Data, Application, Authorize Protocol모형을 설계할 수 있다.

그림 3은 Connection, Data, Application Module을 포함한 유동적인 ICBMS시스템환경을 가정하고 있다. 이 시스템에서는 개념단위의 객체A가 B의 보안모듈을 등록하고 서비스정보를 취득하여 배포하는 과정을 모델

5) 가상머신: 시스템 독립적 가상기기, Java Virtual Machine 환경
 6) DNP: Distributed Network Protocol, 스마트그리드분야의 전력계통 통신프로토콜
 7) ICBMS: IoT, Cloud, BigData, Mobile, Security 분야를 통칭함
 8) N: 기기 인터페이스 구성에 필요한 공유 노드
 9) S: 기기 보안서비스 구성에 필요한 노드
 10) D: 기기 응용프로그램 구성에 필요한 공유 모듈
 11) α : 유니버설미들웨어를 적용한 시스템 모듈의 최대 개수로서 $1 \leq \alpha \leq |N| + |S| + |D|$

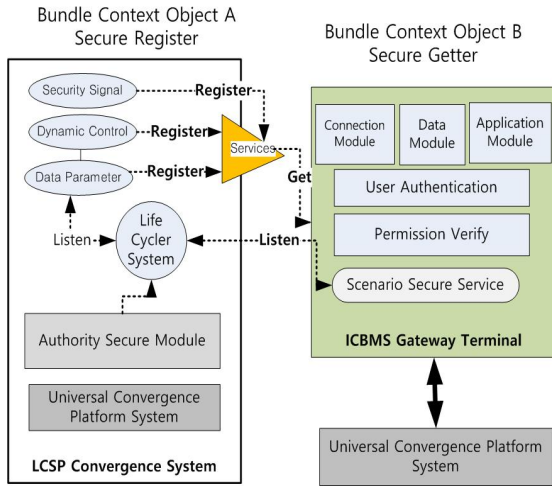


Fig. 3 LCSP Secure Scenario Design

링하였다.

예를 들어 Bundle Context Object A가 IoT응용서비스라고 가정했을 때 A는 Life Cycler에 요구되는 서비스들을 등록한다. Bundle Context Object B에서는 이렇게 등록된 서비스 레퍼런스를 취득하여 배포할 수 있다. 배포단계에서 IoT서비스를 사용하기 위해 필요한 제조와 서비스와 추가되는 요소에 대해서도 실시간으로 보안서비스 모듈을 적용할 수 있을 뿐만 아니라 사용자가 정의한 보안 모듈의 배포도 손쉽게 적용할 수 있다.

이처럼 유니버설미들웨어에서는 Bundle Context Object A와 B가 각각 교환할 수 있는 시나리오 환경을 제공한다. 특히, Authorize Protocol의 경우는 앞서 언급한 ICBMS 환경에서 거대해지고 개념화 되어진 미래의 컴퓨팅 환경에서 요구되는 다양한 인증 시스템을 적용할 수 있다. 또한, 핀테크와 비트코인을 비롯한 추상적인 형태의 요구사항에도 안전하게 대응할 수 있는 시스템을 구축할 수 있다.

III. 결 론

융합보안시스템은 보안중심의 안정적 보안에서 지능적 보안을 확보해야 한다. 융합시스템의 통신모듈과 응용모듈간의 협업 시나리오서비스를 지원도 필수

적이다. 안정성뿐만 아니라 복합적으로 연관된 있는 서비스와 데이터들을 중심으로 개념적으로 연결해야 한다.

본 연구에서는 물리적인 단위로 묶어 전송하는 시스템 구조를 채용하고 안정성과 지능적 연계를 보장하기 위하여 보안시스템을 별도의 레이어로 구성하였다. 별도의 계층을 기반으로 하여 생명주기를 지원하는 유니버설미들웨어를 적용하였다.

유니버설미들웨어기반 보안시스템에서는 데이터포준 모듈, 통신서비스 모듈, 응용서비스 모듈이 각각 보안모듈과 생명주기 형태로 공급되는 신규보안서비스 모듈과 기존의 서비스 모듈간의 시나리오 서비스 구성이 가능하다.

이런 형태의 보안모듈의 개수를 다음과 같이 산정할 수 있다. (단, 보안모듈의 수를 SM, 데이터처리 모듈의 개수를 DM, 응용서비스 모듈 개수를, SM, 통신서비스 모듈을 CM으로 가정한다)

$$\bullet \text{ 구성가능 보안모듈의 개수} = (DM+SM+CM)*SM$$

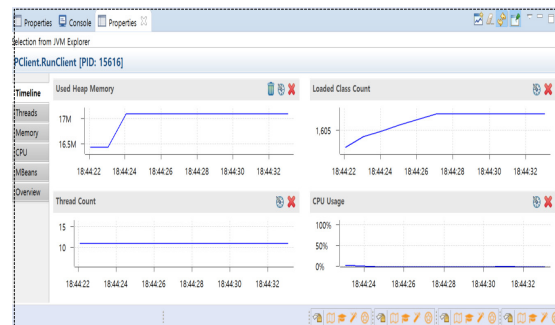


Fig. 4 Monitoring System General Security Client



Fig. 5 Monitoring System for Universal Middleware

그림 4와 그림 5는 동일한 인증 서버에 접속하여 인증서비스를 동일한 조건으로 실행시의 시간별 모니터링 결과를 나타내고 있다.

Table. 1 Rate of System Resources for Timeline.

Item	Universal Middleware	General Purpose Client	Effective Results
Heap Memory	Stable Downturn	Unstable Upturn	Universal Middleware
CPU Usage	Stable Low Flow	Unstable High Flow	Universal Middleware
Loaded Class	Step Upturn	Rate Turn	Universal Middleware
Thread	No Change	No Change	No Relation

표 1에서는 수행시간이 길어질수록 Heap, Thread 사용률, CPU 사용률, 로드된 Class 사용률이 떨어지면서 안정적으로 동작하고 있음을 각각 나타내고 있다.

이 모니터링 결과를 보면 유니버설미들웨어를 사용할 경우 시스템간의 에너지 융합 단말 서비스전송 기술에 적용하는 데 효과적임을 알 수 있다. 결과적으로 미래의 융합서비스의 개념적인 보안 시스템 설계에 필요한 다양성일 고려한 부분이다.

확장성 지원 여부는 보안 시스템에서 적용할 수 있는 분야의 다양성과 확장성 측면에서 보안의 품질을 높일 수 있으며 에너지 융합분야와 관련된 산업기술 응용할 수 있음을 증명하고 있다.

REFERENCES

- [1] J.W. Lee, G.J. Kim, I.J. Hwang, M.W. Yang, H.C. Cho, J.H. Lee "A Study on the Applying Standardized CIM-based model of Power System Application," *40th Conference The Korean Institute of Electrical Engineers(KIEE)*, pp.288-289, July 2009.
- [2] H.J. Lee, D.Y. Seo, "The Study of Dynamic Service Platform for Smart Grid," *Journal of The Korea Knowledge Information Technology Society*, vol.8, no.9, pp.91-100, Dec. 2013.
- [3] OSGi Alliance, OSGi Service Platform Core Specification, Release 4 [Internet]. Available: <https://www.osgi.org/developer> Aug. 2005.
- [4] OSGi Alliance, OSGi Release 5 [Internet]. Available: <https://www.osgi.org/developer> June 2012.
- [5] I. Borthwick, "The Internet of Things: Digital Technology Adoption in the Smart Built Environment," The Institution of Engineering and Technology; Technical Report IET Sector Technical Briefing, Mar. 2015.
- [6] Y.M. Moon, "Demand Response Real Time Pricing Model for Smart Grid Considering Consumer Behavior and Price Elasticity," *Journal of the Korean Operations Research and Management Science Society*, vol.39, no.1, pp. 49-67, Mar. 2014.
- [7] Y. Qian, W. Srisa-an, T. Skotiniotis, J.M. Chang, "Cycle accurate thread timer for Linux environment," *IEEE International Performance Analysis of Systems and Software*, pp.38-44, Nov. 2001.
- [8] J.W. Im, S.H. Kim, D.Y. Kim, "IoT Mashup as a Service: Cloud-based Mashup Service for the Internet of Things," in *Proc. 10th International Conference on Services Computing (SCC)*, pp.462-469. June 2013.
- [9] Y.J. Lim, S.R. Lee, "A Study on the designing mashup manager to support interlock of SaaS platform and mashup tools," *Information & Communications Magazine*, pp.933-934, June 2010.



이해준(Hae-Jun Lee)

1998년 한신대학교 컴퓨터과학과 이학사
 2010년 한국산업기술대학교 컴퓨터공학과 공학석사
 2014년 한국산업기술대학교 컴퓨터공학과 공학박사
 2014-현재 경민대학교 융합소프트웨어과 교수
 ※관심분야 : 유니버설컴퓨팅, 스마트그리드, 사물인터넷, 유니버설미들웨어 보안, 차세대네트워크 서비스



황치곤(Chi-gon Hwang)

1995년 창원대학교 경영학과 경영학사
2004년 광운대학교 정보통신학과 공학석사
2012년 광운대학교 컴퓨터과학과 공학박사
2006년~2015 (주)인찬 연구원
2015년~현재 경민대학교 융합소프트웨어과 교수
※관심분야 : 모바일 클라우드, 멀티미디어 온톨로지, 클라우드 컴퓨팅, 데이터 상호운용



윤창표(Chang-Pyo Yoon)

1998년 광운대학교 전자계산학과 이학사
2001년 광운대학교 컴퓨터과학과 공학석사
2012년 광운대학교 컴퓨터과학과 공학박사
2012년~현재 경기과학기술대학교 컴퓨터모바일융합과 교수
※관심분야 : 모바일 클라우드, 안드로이드 보안, 멀티미디어 온톨로지, 네트워크 프로토콜, 무선 네트워크, 네트워크 보안