유비쿼터스 환경에서 이동단말 및 서비스 보안관리를 위한 u-Middleware

배현철, 김상욱

경북대학교 컴퓨터과학과

u-Middleware for Mobile Device & Security Management based on Ubiquitous Evironment

Hyun-Chul Bae, Sang-Wook Kim

Dept. of Computer Science, Kyungpook National University

요 약

본 논문에서는 유비쿼터스 환경에서 네트워크와 이동단말, 서비스 보안관리 연구를 진행하는데 도움이 되고자 이러한 보안관리를 통합적으로 할 수 있는 미들웨어을 만들게 되었으며 플러그인 형태로 무한한 확장성을 포함하여 정보 수집에서 분석, 정책 설정 및 관리, 위치정보 등의 다양한 기능을 제공한다. 또한 도메인 서버간에 협동을 통해 이동단말의 이동에 대한 다양한 보안관리 연구가 가능하도록 한다.

I. 서론

현재의 네트워크 및 서비스, 단말 보안 관리는 정적으로 설치되어진 네트워크를 구성하는 장비 또는 시스템이다. 유비쿼터스 환경으로 변화하고 있는 지금 이러한 장비와 시스템, 서비스의 규모가 크며, 이동성을 가지는 장비의 추가로 인하여 정확한 세부 정보를 파악 및 위치파악이 어렵다. 그리고, 네트워크 구성 또는 구성 요소의 변동이 심하며, 구성 요소의 종류가 매우 다양하기 때문에 공통적인 방식으로 접근하기가 불가능하다. 때문에 기존의 네트워크 관리 방식과 도구로는 효과적인 결과를 기대할 수 없다. 세부 정보의 결여로 효과적인 제어도 쉽지 않다. 특히 네트워크에 대한 긴급한 제어가 요구되더라도 다양한 기종과 각각에 대해 접근해야 하는 절차적 복잡성으로 인해 적절한 대응이 어렵다. 때문에, 네트워크 보안 관리와 더불어 이동단말 보안관리, 제공하는 서비스에 대한 보안관리를 효과적으로 수행하기 위해서는 다양한 구성 요소에 일괄적으로 접근할 수 있는 방법이 필요하다. 보안 관리에서 관리하고자 하는 구성 요소는 기본적으로 라우터, 일반 호스트, 방화벽, 센서 등의 정적인 것과 PDA, 휴대폰, 스마트폰 등의 이동단말 그리고, 서비스등이 있다.

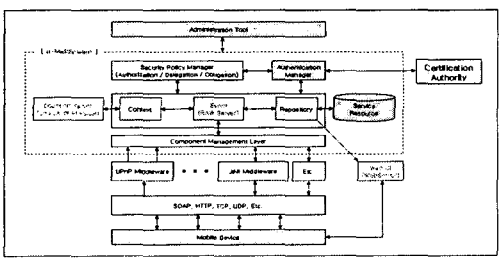
보안 관리에는 다양한 구성 요소와 이들 사이의 복잡한 관계로 구성되어 있다. 때문에 그것을 관리하고 제어하기 위해서는 자동화된 관리 메커니즘이 요구되며, 그러한 메커니즘에 의한 실제적인 구성 요소에 대한 접근과 제어를 위해서는 일정 수준의 세부 정보가 필요하며 종합적으로 관리할 수 있는 시스템이 필요하다. 이에 2장에서 이러한 관리

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음.

를 위한 u-Middleware의 구조와 동작흐름에 대해서 얘기하며, 3장에서 유비쿼터스 환경에서의 통합 보안 관리를 위한 u-Middleware의 구성과 역할에 대해 설명하고, 4장에서 u-Middleware을 구성하는 각 시스템에 대한 것을 소개하며, 5장에서 결론을 맺는다.

II. u-Middleware의 구조

유비쿼터스 환경은 기존의 네트워크 환경과는 비교할 수 없을 만큼의 많은 데이터들을 처리해야 한다. 이러한 데이터들은 표준화 구조를 가지는 데이터 이외에 해당 장치의 제조사나 개발자에 임의로 만든 구조를 가지 데이터들도 존재하게 된다. 대량의 데이터와 표준화/비표준화 데이터에 대해서 통합적으로 관리하기 위해서는 이를 각각의 계층을 두어 처리하는 것이 필요하다. 이에 본 논문에서 제안하는 시스템은 LOG계층, EVENT 계층 이렇게 2개의 계층으로 구분하여 데이터를 분석하고 처리한다. 우선 LOG 계층은 해당 도메인내에 각종 장치나 센서 등의 오브젝트로부터 표준/비표준화된 데이터를 무조건 적으로 수신 및 분석처리하며, 수신 및 분석된 데이터를 기반으로 데이터베이스에 해당 장치에 대한 정보를 포함하여 관리에 필요한 정보를 추가하여 추후 구체적인 정보를 조회할 있도록 구성되어 기록한다. EVENT 계층은 이렇게 구체적으로 기록되어진 것에 대하여 이벤트화하여 중복되거나 통보되지 않아도 되는 정보에 대해서 필터링과 데이터 량을 줄이는 등의 역할을 수행하는 계층이며, 또한 u-Middleware은 이러한 2개 계층을 기준으로 그림 1과 같은 형태로 구조를 가지며 동작한다.



<그림 1> u-Middleware 구조

전체 4개의 세부 시스템으로 구성되어 있으며 각 시스템은 메시지를 이용하여 서로간의 통신을 수행한다.

u-Middleware는 기본적으로 제공되는 시스템에 종속적이지 않고 플러인 형태의 확장성을 제공하므로써 다양한 외부 시스템과의 연동이 용의한 구조를 가지고 있다.

III. 구성 및 역할, 메시지

3.1 구성 및 역할

전체 시스템의 구성 및 역할은 다음과 같다.

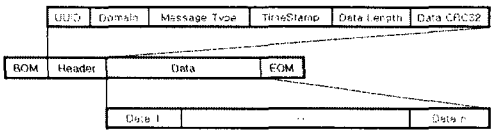
<표 1> 시스템 구성 및 역활

종류	역할
u-Middleware	이동 단말 및 서비스 시스템, 네트워크 장치로부터 발생되는 다양한 형태를 가지는 데이터를 UCMF로 변환 및 UCMF형식의 정리된 데이터를 기반으로 Event 추출/생성 및 Administrator Tool로 전송
Administrator Tool	Location Server 및 u-Middleware를 관리하며 정책 설정 및 관리, 각종 정보 분석 및 관리
Location Server	각 u-Middleware와 연결된 시스템들간에 위치 확인을 위한 정보관리
Authentication Server	인증 및 위임처리를 위한 서버로써 인증 및 위임관련 정보 관리

Authentication Server의 경우 자체적으로 개발한 시스템을 적용하거나 공인된 인증시스템과 연동할 수 있도록 u-Middleware에서 제공한다. 이에 본 논문에서는 공인된 인증시스템을 사용하므로 이에 대한 것은 제외한다.

3.2 UCMF

UCMF은 u-Miidleware Common Message Format의 약자로써 u-Middleware에서 통합적인 보안관리를 함에 있어 필요한 데이터를 전송하는데 최소한의 신뢰성 보장과 표준화를 위하여 메시지 형식을 정의하였으며, 일반적인 문자열형태로 구성되어 가변길이를 가지는 구조로 구성되어 있다. 메시지 구조는 그림2와 같은 형태로 구성되어 진다.



<그림 2> UCMF 구조

전체적인 구조는 메시지의 시작을 나타내는 BOM 필드, 메시지의 끝을 나타내는 EOM 필드과 메시지 정보를 담고 있는 헤더 필드, 관련 데이터가 담겨 있는 데이터 필드 이렇게 4가지 부분으로 나뉘어진다.

헤더 필드는 각 장치나 이동단말에서 발생한 데이터를 고유한 UUID(Universal Unique IDentification)와 소속된 도메인 정보, 보내는 메시지의 종류, 메시지를 전송할 당시의 msec 단위의 시간정보, 데이터의 총길이, 데이터에 대한 CRC32 값으로 구성된다. 또한 메시지 종류는 다음과 같다.

<표 2> 메시지 종류

종류	설명
N	일반 메시지
S	시스템 메시지 (ALIVE, PING/PONG 등)
M	모니터링 메시지
C	제어 메시지
0	실시간 메시지
1-9	우선 순위 메시지 (Reserved)
V	바이러스나 웜, 해킹 등에 의한 가상 공격 메시지 (Reserved)

데이터 필드 부분은 일정한 형식이 없으며 여러 개의 데이터를 구분하여 적재하여야 하는 경우 정의된 구분자를 이용하여 구분하여 하나의 데이터로 생성하여 적재하면 된다. UCMF는 u-Middleware 내에서 모든 데이터 전송에 사용되며 사용되는 데이터는 UCMF 형식으로 변환되어 메시지 형태로 전송 되어진다.

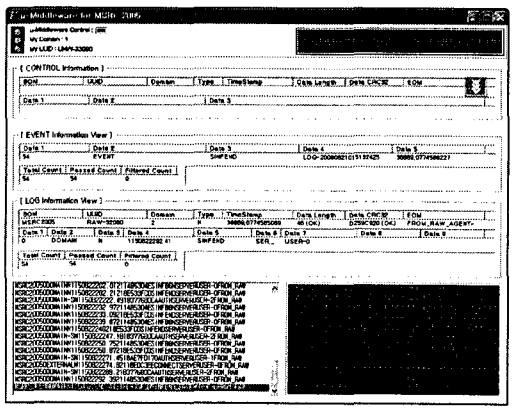
3.3 보안관리를 위한 정책처리

XML기반의 정책을 통해 u-Middleware와 연결된 다양한 장치와 시스템들에 대해서 일률적인 정책을 설정가능하며, 이러한 정책은 u-Middleware에서 연결된 장치에 맞는 Rule-Set이나 정책형태에 맞도록 자동 변환되어 해당 시스템에 적용된다. 또한 u-Middleware에 적재된 정책에 대해 주기적인 관리를 통해 폐기와 갱신 작업을 수행한다.

IV. 구현

4.1 u-Middleware

현재 유비쿼터스 환경을 위하여 상용화된 각종 센서를 비롯하여 장비들은 표준화된 데이터 형식보다는 제조사 자체의 형식으로 데이터를 전송하는 구조를 가지고 있다. 이에 표준화되지 않는 데이터를 수신하고 UCMF 메시지로 변환을 수행하며 데이터 필드에 수신한 데이터를 재가공한 내용이 적재된다. 헤더 필드부분에는 UUID 및 소속된 도메인 등이 정보가 기록된다. 수신한 데이터에 대해 분석 및 변환과정에서 문제가 있는 경우 Administrator Tool 에 이를 알리며 Event 를 생성하여 전송한다. Location Server와 연결되면 자신의 UUID와 소속 도메인 정보 등을 전송하여 위치정보를 등록하며 이동하거나 종료되는 경우에도 Location Server에 상태와 이동에 따른 정보를 등록한다.



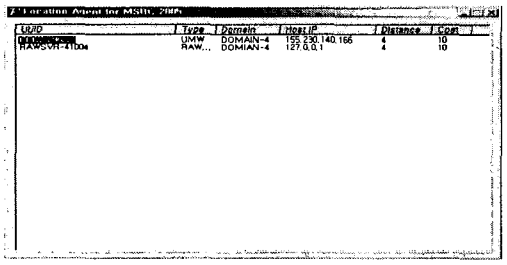
<그림 3> u-Middleware

UCMF 메시지를 분석하여 DB에 LOG 형태로 기록하며 전달 받은 메시지에 대해서 설정된 정책에 따라 변환 및 Event 메시지를 생성한다. 이때 생성된 Event 정보는 DB에 기록되며 또한, Administrator Tool에서 전

달 받은 정책을 분석하고 자기 자신과 연결된 네트워크 장치나 서비스 시스템, 이동단말 등에 정책을 적용한다. 정책 적용 기능 이외에 LOG와 Event에 대해 Filtering 기능을 이용하여 반복적이거나 필요 없는 정보에 적용하여 Filtering을 수행한다. Filtering 정보 또한 Administrator Tool에서 전달 받은 것과 자체적인 학습에 의해 결정된 것으로 나뉘어 진다. 자체적인 학습에 의한 처리 부분은 플러그인 기능을 이용하여 원하는 시점에서 원하는 학습방법을 통한 Filtering 정보를 적용할 수 있다.

4.2 Location Server

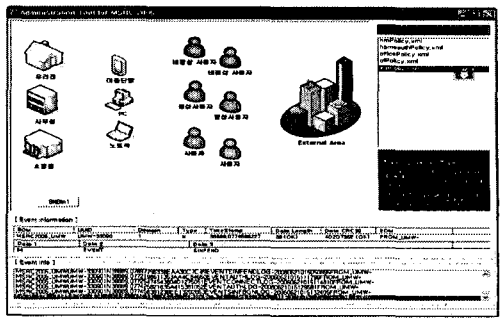
도메인 내의 시스템들에 대한 위치정보를 관리한다. u-Middleware와 연동하여 위치정보 관리를 처리하며 Administrator Tool에는 등록된 정보를 조회하고 조회한 정보를 이용하여 각 시스템에 접속 및 관리를 수행한다. 또한 각 시스템에서 위치정보 등록 시에 거리와 비용 개념을 도입하여 Routing 처리가 가능하도록 확장성을 제공한다.



<그림 4> Location Server

4.3 Administrator Tool

관리를 위한 시스템으로써 정책 및 필터링 정보 설정 및 조회/관리를 수행할 수 있으며, Location Server와 연결하여 각 시스템의 정보를 요청하여 전달 받은 뒤 이를 시각화하여 보여주는 기능과 더불어 미들웨어에서 전달받은 Event 정보에 대해 분석을 수행하며 분석된 내용을 리포팅한다.



<그림 5> Administrator Tool

5. 결론

본 논문에서 연구되어진 u-Middleware는 유비쿼터스 환경에서 서비스 제공 시스템과 네트워크 장치, 이동단말에서 발생할 수 있는 각종 상황과 이에 따른 보안관리, 생성되는 데이터 등을 종합적으로 관리할 수 있는 시스템이다. 또한, 여러 개의 도메인과 여러 개의 u-Middleware를 동작시킬 수 있으므로 실제 환경에서 발생할 수 있는 애로사항에 적극적으로 대처할 수 있도록 구성하였다. 추후 GPS와 다양한 위치정보 파악 기술과 더불어 안정화와 구체적인 요구사항 정리 과정을 거쳐 다양한 응용 시스템과 더불어 실제 장치와의 연동, 보안관리 요소 추가, 관리를 위한 사용자 인터페이스의 시각화 등 확장을 시킬 예정이다

[참고 문헌]

[1] Anind K. Dey and Gregory D. Abowd , "The Context Toolkit: Aiding the Development of Context-Aware Applica- tions", In the Workshop on Software Engineering for Wearable and Pervasive Computing , Limerick, Ireland, June 6, 2000.

[2] David R. Morse, Anind K. Dey and Stephen Armstrong, Workshop Organizers, "The What, Who, Where, When and How of Context-Awareness ", Workshop abstract in the Proceedings of the 2000 Conference on Human Factors in Computing Systems (CHI 2000), The Hague, The Netherlands, April 1-6, 2000, p. 371.