유비쿼터스 환경에서 이동단말 및 서비스 통합 보안관리를 위한 u-Ware 시스템

배현철 김상욱
경북대학교 컴퓨터과학과
{hcbae, swkim}@woorisol.knu.ac.kr

u-Ware System for Mobile & Service Total Security Management based on Ubiquitous Evironment

HyunChul Bae, SangWook Kim
Dept. of Computer Science, Kyungpook National University

요 약

본 논문에서는 유비쿼터스 환경에 산재되어 있는 다양한 센서와 이동단말, 서비스를 제공하는 서버등에 대해 통합적으로 보안관리를 수행하는 시스템을 제안함과 동시에 플러그인 형태로 무한한 확장성을 포함하여 통합 보안관리를 위한 정보 수집에서 분석, 정책 설정 및 관리, 위치정보 등의 다양한 기능을 제공한다. 또한 도메인 서버간에 협동을 통해 이동단말의 이동에 대한 다양한 보안관리 연구가 가능하도록 하며, 통합 보안관리 도구를 통해 이질적인 환경에서 일괄적으로 관리를 수행하고 모니터링하며 시각화를 통해 보안관리 효율을 높일 수 있는 환경을 제안한다.

1. 서론

기존 네트워크 기반에서 통합 보안관리는 정적으로 구성되어진 장비 또는 시스템을 대상으로 한다. 유비쿼터스 환경으로 변화하고 있는 지금 기존의 환경은 이동성을 가지는 장치에 대해하여 정확한 세부 정보를 파악 및 위치파악이 어려우며, 이동단말과 서비스에 대한 통합 보안관리가 요구되어지고, 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 이동 단말과 제공하는 서비스에 대한 보안관리를 효과적으로 수행하기 위해서는 다양한 구성 요소에 일괄적으로 접근할 수 있는 방법이 필요하다. 보안 관리에서 관리하고자 하는 구성 요소는 기본적으로 네트워크 장비를 비롯하여 다양한 센서 등의 정적인 것과 PDA, 휴대폰, 스마트폰 등의 이동단말 그리고 서비스를 제공하는 서버등이 있다.

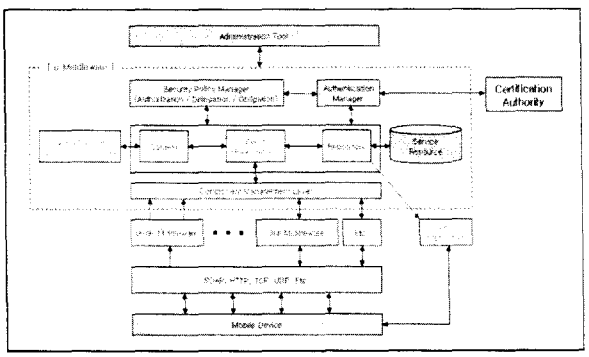
보안 관리에는 다양한 구성 요소와 이들 사이의 복잡한 관계로 구성되어 있다. 때문에 그것을 관리하고 제어하기 위해서는 자동화된 관리 메커니즘이 요구되며, 그러한 메커니즘에 의한 실제적인 구성 요소에 대한 접근과 제어를 위해서는 일정 수준의 세부 정보가 필요하며 통합적으로 관리할 수 있는 시스템이 필요하다. 이에 2장에서 이러한 관리를 위한 u-Ware 시스템의 구조와 동작흐름에 대해서 얘기하며, 3장에서 유비쿼터스 환경에서의 통합 보안 관리를 위한 u-Ware 시스템의 구성과 역할에 대해 설명하고, 4장에서 u-Ware 시스템을 구성하는 각 시스템에 대한 것을 소개하며, 5장에서 결론을 맺는다.

2. u-Ware 시스템의 구조

유비쿼터스 환경은 기존의 네트워크 환경과는 비교할 수 없을 만큼의 많은 데이터들을 처리해야 한다. 이러한 데이터들은 표준화된 형식을 가지는 데이터와 해당 장치의 제조사나 개발자가 임의로 만든 구조를 가지 데이터들이 함께 존재하게 된다. 이러한 대량의 데이터와 표준화/비표준화 데이터에 대해서 통합적으로 관리하기 위해

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음.

서는 이를 각각의 계층을 두어 처리를 함으로써 효율적으로 대량의 데이터 처리가 가능하다. 이에 본 논문에서 제안하는 시스템은 LOG계층, EVENT계층 이렇게 2개의 계층으로 통해 데이터를 분석하고 처리한다. 우선 LOG 계층은 해당 u-Ware 시스템이 속해 있는 도메인내에 u-Ware 시스템과 연결되어진 다양한 센서와 서비스 서버 그리고, 서비스를 요청하고 제공받는 이동단말 등의 다양한 대상으로부터 표준/비표준화된 데이터를 수신 및 분석 처리하며, 수신 및 분석된 데이터를 기반으로 데이터베이스에 해당 시스템에 대한 정보를 포함하여 관리에 필요한 정보를 추가하여 캡슐화 후에 DB에 기록한다. EVENT 계층은 이렇게 기록되어진 LOG에 대하여 중복되거나 통보되지 않아도 되는 정보에 대해서 필터링 처리와 더불어 관리자 도구 및 인접 u-Ware 시스템들간에 협동처리를 위한 EVENT를 생성하여 서로간에 전달하는 역할을 수행하며 하는 계층이며, 또한 u-Ware 시스템은 이러한 2개 계층을 기준으로 그림 1과 같은 형태로 구조를 가지며 동작한다. 이외에 관리 도구에서 전달받은 정책은 위의 2개 계층과는 별도로 분석 및 처리를 하여 대상 시스템에 맞는 형태의 Rule로 변환을 거쳐 적용 및 갱신/폐기 등 관리가 되어진다.



<그림 1> u-Ware 시스템 구조

각 세부 시스템 간에는 UCMF라는 자체적인 메시지 단위로 서로간의 통신과 필요한 데이터 전송을 수행하며 플러인 형태의 확장성을 제공하므로써 다양한 외부 시스템과의 연동이 용의한 구조를 가지고 있다.[1][2]

3. 구성 및 역할, 메시지

3.1 구성 및 역할

전체 시스템의 구성 및 역할은 표1과 같이 크게 4가지로 구분되어지며, 각각의 서버와 도구는 동일 도메인 내에 여러 개가 존재하거나 하나의 u-Ware 시스템을 통해 여러 개의 도메인을 관리할 수 있다.

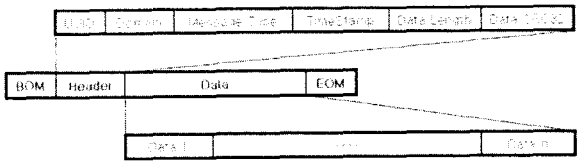
<표 1> 시스템 구성 및 역할

종류	역할
도메인 서버	이동 단말 및 서비스 서버, 센서 등에서 발생되는 비표준/표준형식 데이터를 UCMF로 변환 및 UCMF형식의 정리된 데이터를 기반으로 EVENT 추출/생성 및 통합 보안관리 도구로 전송
통합 보안 관리도구	위치정보 관리서버 및 u-Ware 시스템을 관리하며 정책 설정 및 관리, 각종 정보 분석 및 관리
위치정보 관리서버	각 u-Ware 시스템과 연결된 시스템들간에 위치 확인을 위한 정보관리
인증/위임 서버	인증 및 위임처리를 위한 서버로써 인증 및 위임관련 정보 관리

u-Ware 시스템에서 도메인 서버가 모든 데이터의 분석 및 처리를 포함하여 를 수행하며, 인증/위임 서버의 경우 자체적으로 개발한 시스템을 적용하거나 공인된 인증시스템과 연동할 수 있도록 되어 있으며, 본 논문에서는 공인된 인증시스템을 사용하므로 이에 대한 것과 최종 사용자에게 제공되어지는 인터페이스인 WEB 기반에 설정부분은 언급을 제외한다.

3.2 UCMF

UCMF은 u-Ware Common Message Format의 약자로써 u-Ware 시스템에서 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-Ware 시스템 내에서 모든 데이터 전송에 사용되며 사용되는 데이터는 UCMF 형식으로 변환되어 메시지 형태로 전송 되어진다.

3.3 보안관리를 위한 정책처리

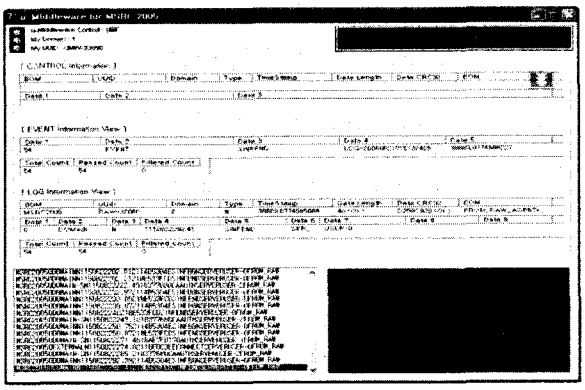
XML기반의 정책작성과 더불어 시간만료 개념을 도입하여 통합 보안관리 도구에서 u-Ware 시스템과 연결된 다양한 장치와 시스템들에 대해서 추상적인 형태의 정책 작성 후 일률적인 정책 설정 및 갱신/삭제 등의 관리가 가능하며, 이러한 정책은 u-Ware 시스템에서 연결된 장치가 요구하는 형태의 최종 Rule 형태에 맞도록 도메인 서버에서 자동 변환되어 연결되어진 해당 시스템에 적용된다.[3][4]

또한 도메인 서버에 적재된 정책은 자체적인 학습과 관리자의 설정에 의한 강제적 관리, 주기적 관리등의 다양한 방법으로 통합 보안관리 도구와 인접한 u-Ware 시스템간에 협동하여 폐기와 갱신 작업을 수행한다.

4. 구현

4.1 도메인 서버

현재 유비쿼터스 환경을 위하여 상용화된 각종 센서를 비롯하여 장비들은 표준화된 데이터 형식보다는 제조사 자체의 형식으로 데이터를 전송하는 구조를 가지고 있다. 이에 LOG 계층에서 비표준/표준형태의 데이터를 수신하고 UCMF 메시지로 캡슐화 과정을 수행하며 데이터 필드에 수신한 데이터 내용이 적재된다. 헤더 필드부분에는 UUID 및 소속된 도메인 등이 정보를 기록하고 DB에 LOG로 기록을 남기게 된다. EVENT 계층에서는 수신한 데이터에 대해 분석과정에서 데 EVENT를 생성하여 통합 보안관리 도구로 전송한다. 위치정보 관리서버와 연결되면 자신의 UUID와 소속 도메인 정보 등을 전송하여 위치정보를 등록하며 이동하거나 종료되는 경우에도 위치정보 관리서버에 상태와 이동에 따른 정보를 등록 및 갱신한다.

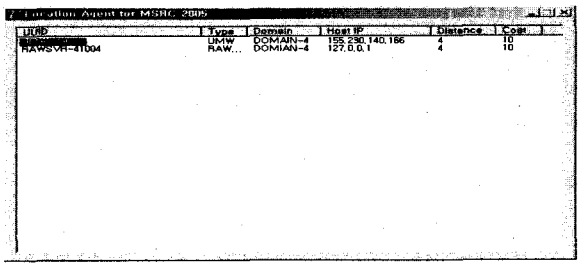


<그림 3> 도메인서버

통합 보안관리 도구에서 전달 받은 정책을 분석하고 자기 자신과 연결된 네트워크 장치나 서비스 시스템, 이동단말등에 정책을 적용한다. 정책 적용 기능 이외에 LOG와 EVENT에 대해 필터링 기능을 이용하여 반복적이거나 현 시점에서 보안관리를 함에 있어 제외대상에 포함된 경우에 해당 정보를 제외한다. 필터링 정보 또한 통합 보안관리 도구에서 전달 받은 것과 자체적인 학습에 의해 결정된 것으로 나뉘어진다. 자체적인 학습에 의한 처리 부분은 플러그인 기능을 이용하여 원하는 시점에서 원하는 학습방법을 통한 필터링 정보를 적용할 수 있다.

4.2 위치정보 관리서버

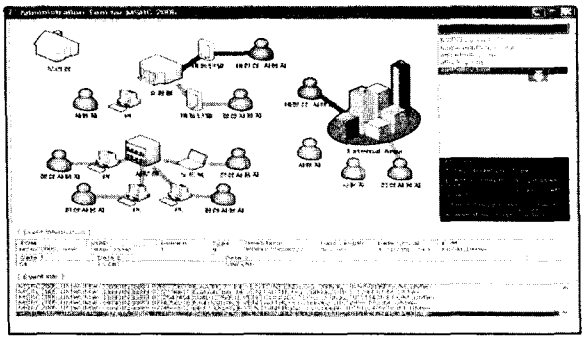
도메인 내의 시스템들에 대한 위치정보를 관리한다. u-Ware 시스템과 연동하여 위치정보 관리를 처리하며 통합 보안관리 도구에는 등록된 정보를 조회하고 조회한 정보를 이용하여 각 시스템에 접속 및 관리를 수행한다. 또한 각 시스템에서 위치정보 등록 시에 거리와 비용 개념을 도입하여 라우팅 처리가 가능하도록 확장성을 제공한다.



<그림 4> 위치정보 관리서버

4.3 통합 보안관리 도구

통합 보안관리를 위한 도구로써 정책과 필터링 정보를 제외한 나머지 정보는 그림 5와 같이 시각적으로 표현하여 관리 효율을 높여준다.



<그림 5> 통합 보안관리 도구

또한, 도구에서 처리할 수 있는 일은 다음과 같다.
- 정책 작성 및 조회/관리
- 필터링 정보 설정 및 조회/관리
- 위치정보 관리서버와 연결하여 각 시스템의 위치확인
- 연결된 시스템과 이동단말, 사용자들의 상태 모니터링

시각화하여 보여주는 기능과 더불어 도메인서버에서 전달받은 EVENT 정보에 대해 분석을 수행하며 분석된 내용을 다양한 형태로 리포팅한다.

5. 결론

본 논문에서 연구되어진 u-Ware 시스템은 유비쿼터스 환경에서 서비스 제공 시스템과 네트워크 장치, 이동단말에서 발생할 수 있는 각종 상황과 이에 따른 보안관리, 생성되는 데이터 등을 통합 관리할 수 있는 시스템이다. 또한, 여러 개의 도메인에서 운영이 가능하며, 인접한 u-Ware 시스템들간에 연동은 하여 통합 관리가 가능하므로 실제 환경에서 발생할 수 있는 다양한 문제점에 효율적으로 대처할 수 있도록 구성하였다. 추후 인접 u-Ware 시스템간에 협동처리를 수행함에 있어서 효율적이며, 스스로 학습에 의한 최적화된 보안관리를 할 수 있는 방안에 대하여 추가적으로 연구와 더불어 보안관리 요소 추가, 관리를 위한 사용자 인터페이스의 시각화 등 확장하여 연구할 것이다.

[참고 문헌]

[1] Michael J. Covington, Prahlad Fogla, Zhiyuan Zhan, Mustaque Ahamad: A Context-Aware Security Architecture for Emerging Applications. ACSAC 2002: 249-260.

[2] Jalal Al-Muhtadi , Anand Ranganathan , Roy Campbell , M. Dennis Mickunas, Cerberus: A Context-Aware Security Scheme for Smart Spaces, Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, p.489, March 23-26, 2003

[3] Michael J. Covington, Matthew J. Moyer, and Mustaque Ahamad. Generalized role-based access control for securing future applications. In Proceedings of the 23rd National Information Systems Security Conference(NISSC), pages 40-51, Baltimore, Maryland, USA, October 2000.

[4] Matthew J. Moyer and Mustaque Ahamad. Generalized role based access control. In Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS), Mesa, Arizona, USA, April 2001.