논문 2006-01-09

여러 임베디드 장치의 통합 관리를 위한 프레임워크 개발

(A Framework Development for Total Management of Various Embedded Devices)

배 현 철, 김 상 욱*
(HyunChul Bae, SangWook Kim)

Abstract : in this paper, we propose the integrated security management framework supporting the trust for the ubiquitous environments. The proposed framework provides the gathering and analysis of the security related information including the location of mobile device and then dynamically configures the security policy and adopts them. More specially, it supports the authentication and delegation service to support the trusted security management for the ubiquitous networks. This system also provides the visible management tools to give the convenient view for network administrator.

Keywords : ubiquitous, embedded, policy, security, distributed, monitoring

Ⅰ. 서 론

기존 네트워크 기반에서 통합 보안 관리는 정적으로 구성되어진 장비 또는 시스템을 대상으로 하며, 이동성을 가지는 장치에 대해하여 정확한 세부 정보를 파악 및 위치파악이 어려움이 있다. 또한, 유비쿼터스 환경으로 변화하고 있는 지금 이동단말과 서비스, 적시적소에 설치되고 사용되어지는 여러 임베디드 장치, 기존에 사용되던 장치들에 대한 통합 보안관리가 요구되어지고, 네트워크 구성 또는 구성 요소의 변동이 심하며, 구성 요소의 종류가 매우 다양하기 때문에 공통적인 방식으로 접근하기가 불가능하다. 때문에 기존의 보안관리 방식과 도구로는 효과적인 결과를 기대할 수 없다. 세부 정보의 결여로 효과적인 제어도 쉽지 않다. 특히 대상 환경에 대한 긴급한 제어가 요구되더라도 다양한 기종과 각각에 대해 접근해야 하는 절차적 복잡성으로 인해 적절한 대응이 어렵다. 임베디드 장치와 일반적인 하드웨어 장치에 대한 보안 관리와 더불어 이동 단말과 제공하는 서비스에 대한 보안 관리를 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 서버, 특정 환경 및 기능에 최적화된 임베디드 장치 등이 있다. 이러한 장치들과 이러한 장치들을 연결시켜주는 네트워크에 대한 보안 관리를 위해서는 다양한 구성 요소와 이들 사이의 복잡한 관계로 구성되어야 한다. 때문에 그것을 관리하고 제어하기 위해서는 자동화된 관리 메커니즘과 시스템이 요구되며, 그러한 메커니즘에 의한 실제적인 구성 요소에 대한 접근과 제어를 위해서는 일정 수준의 세부 정보가 필요하며 통합적으로 관리와 더불어 대량의 데이터를 안전하고 고속으로 처리하며, 종합적으로 문제점과 상태를 관제하고 관리하고 할 수 있는 프레임워크 개발이 필요하다. 이에, 본 논문에서는 기존의 장치와 더불어 여러 임베디드 장치에 효율적으로 통합 보안 관리를 수행할 수 있는 프레임워크를 제안하며, 프로토타입 수준의 u-Ware 시스템의 전체적인 소개와 함께 설계된 시스템의 구성, 구현 결과를 소개한다. 이에 2장에

* 교신저자(Corresponding Author)
논문접수 : 2006. 10. 24.
배현철, 김상욱 : 경북대학교
※본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음 (IITA-2006-C1090-0603-0026)

서 이와 관련된 관련연구와 요구사항에 대해서 언급하며, 3장에서 유비쿼터스 환경에서의 다양한 장비들과 여러 임베디드 장치에 대한 통합 보안 관리를 위하여 제안하는 u-Ware 시스템의 대해 설명하고, 4장에서 프로토타입으로 구현된 u-Ware 시스템을 소개하며, 5장에서 결론을 맺는다.

Ⅱ. 관련연구 및 요구사항

1. 관련 연구

1.1. 트래픽 추이 분석

네트워크 장비로부터 일정시간이나 간격동안의 트래픽 정보를 수집, 분석하여 정상 트래픽 패턴과 비교를 함으로써 현재 트래픽의 이상 조기에 탐지한다. 이러한 트래픽 분석 방식은 트래픽 양(Volume)과 플로우(Flow) 분석[7-8]으로 나누어진다 트래픽 양 분석은 라우터와 같은 네트워크 장비로부터 SNMP(Simple Network Management Protocol)을 이용하여 IP계층의 트래픽 양과 관련된 정보를 수집하며, 시간 또는 일자별로 설정된 변동 임계치(Variation threshold value)와 비교하여 이상 트래픽을 탐지해낸다. 이러한 방식의 경우 서비스 거부 공격이나 웜과 같은 대량의 이상 트래픽 발생을 빠르게 탐지할 수 있으나 서비스 프로토콜로 상세한 공격정보를 알 수 없기 때문에 별도의 트래픽 분석을 위한 장비가 추가적으로 필요하다는 단점이 있다. 플로우 분석은 송신자에서 수신자로의 일련의 단방향성 패키의 흐름을 분석하는 것이다. 플로우는 서비스 접속 주소(송신자 주소, 송신자 포트 번호, 수신자 주소, 수신자 포트 번호), 호스트 주소(송신자 네트워크 주소, 수신자 네트워크 주소) 및 AS번호(송신자의 AS 번호, 수신자 AS 번호)등의 정보를 포함하고 있다. 이러한 정보를 기반으로 서비스(포트 번호), 프로토콜(TCP, UDP, ICMP 등), 패킷 사이즈 분포, 출발지 및 목적지 주소[9-10]등의 통계지표를 생성한 후 정상적인 트래픽 패턴과 비교하여 이상 트래픽 탐지한다. 플로우 분석 방식은 트래픽 양 분석 방식에 비해 이상 트래픽을 보다 상세하게 분석, 탐지할 수 있는 장점이 있으나 방대한 규모의 데이터 축적과 분석 시스템의 구축에 많은 비용이 들며, 플로우 정보 수집으로 인해 해당 네트워크 장비의 성능을 저하시킬 수 있는 단점이 있다. 이상 언급한 네트워크 트래픽 추이분석 방식은 웜의 발생으로 인해 대량의 이상 트래픽이 발생하는 것을 탐지하기 용이하다는 장점이 있다. 그러나 정상적인 트래픽의 폭주(Congestion) 현상과 웜 발생으로 인한 트래픽의 이상변화를 구별하기가 어렵다는 문제점이 있다. 즉 탐지 오류(False Positive)가 발생하기 쉬워 보안 관리자의 부담이 커지고, 자세한 트래픽 분석을 위한 별도의 시스템 운용이 필요 하는 문제가 있다.

1.2 로그간 상관관계 분석

네트워크상에서 운용되는 다양한 보안 장비(N-IDS, IPS, 방화벽 및 VPN 등)는 개별적인 형태의 침입 탐지/차단 로그를 생성한다. 이러한 로그 데이터들 간의 상관관계를 분석하여 공격을 신속하게 탐지하는 방법에 대한 연구가 활발하다. 로그간 상관관계 분석 기법은 분산되어 있는 여러 장비들로부터 로그정보를 수집하여 이들 간의 상관성을 분석함으로써 위험 발생 가능성을 보다 정확히 탐지하고, 위협요소를 예측하며 임박한 위협 경보를 신속히 전달하는 것을 목표로 하고 있다. 이와 같은 기능을 지원하기 위해서는 네트워크상의 주요 관리대상 시스템들에 위협을 탐지할 수 있는 센서기능을 갖는 에이전트(Agent)를 두어야 하고, 서로 상이한 형태의 로그 포맷을 통일된 형태로 변환하여 관리해야 한다. 이와 같은 개념으로 구현한 제품이 대표적인 제품[11]으로 EMS이 있으나 정책설정 과정이 복잡하므로 많은 시간이 소요된다. 또한 다양한 로그를 기반으로 판단한 문제의 신뢰성 검증이 불가능하며, 문제발생시 대책과 조치가 전적으로 보안 관리자의 판단에 의존해야 하는 단점이 있다.

2. 요구사항

일반적인 네트워크상의 노드 간에 통신이나 분산 시스템에서 보안은 사용자나 개체에 대한 신뢰를 할 수 있는지 또는 주고받는 메시지를 신뢰할 수 있는지에 관한 인증, 주고받는 메시지에 대한 내용을 비밀로 하는 기밀성, 메시지가 통신 중간에 변질이 되지 않았음을 검증하는 무결성과 탐지되어진 많은 데이터을 어떻게 효율적으로 처리할 것인가에 관한 가용성의 관점으로 많이 다루어진다[5]. 유비쿼터스 환경에서 통합 보안 관리는 무선 통신을 기본으로 개체 간에 통신을 하고, 모든 개체에 컴퓨팅이 가능한 형태의 임베디드 시스템으로 될 것이라는 비전에 따라 기본의 보안과는 크게 다르지는 않지만, 추가적인 고려사항이나 제약점이 생길 것이다. 따라서 유비쿼터스 환경에서의

보안 관리는 대규모의 데이터를 어떻게 관리할 것인가와 더불어 인증, 기밀성, 무결성, 시각화 등의 기능을 갖춘 종합적인 관리 환경을 요구한다. 또한 임베디드라는 하드웨어적 환경이 시스템을 구동할 수 있는 환경을 제한할 수 있으므로 해당 시스템의 모듈화를 통하여 환경에 최적화된 임베디드 시스템을 구성할 수 있어야하며, 제한적 범위 내에서 소프트웨어적인 다양한 확장성을 통하여 하드웨어 및 소프트웨어에 대한 유지비용 보수를 최소화 할 수 있어야 한다.

Ⅲ. u-Ware 시스템

1. 시스템 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 위해서는 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 도메인 내에 u-Ware 시스템과 연결되어진 다양한 센서와 서비스 서버 그리고, 서비스를 요청하고 제공받는 이동단말 등의 다양한 대상으로부터 표준/비표준 화된 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 시스템들 간에 협동처리를 위한 EVENT를 생성하여 서로 간에 전달하는 역할을 수행하며 하는 계층이며, 또한 u-Ware 시스템은 이러한 2개 계층을 기준으로 그림 1과 같은 형태의 프레임워크로 구성되어 있다. 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 된다.

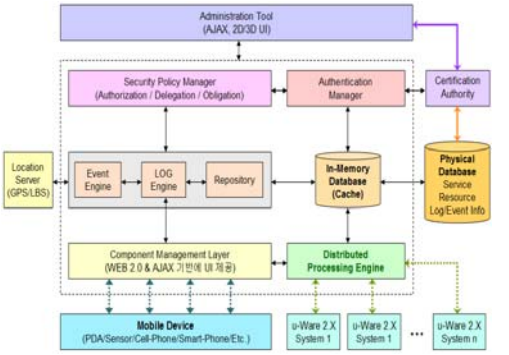

그림 1. u-Ware 시스템 프레임워크
Fig 1. u-Ware System Framwork

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

2. 구성 및 역할

u-Ware 시스템의 전체 구성 및 역할은 표 1과 같이 크게 7가지로 구분되어지며, 서로 간에 UCMF라는 메시지를 통하여 관련 정보를 주고받는다. 또한 u-Ware를 구성하는 시스템은 동일 도메인 내에 여러 개가 존재하거나 하나의 u-Ware 시스템을 통해 여러 개의 도메인을 관리할 수 있다.

2.1 컴포넌트 관리모듈

Component Management Layer는 u-Ware와 연결되는 이동단말, 센서 등의 다양한 기기가 사용하는 통신방식에 대해서 통합적으로 관리하고 정보를 받아들이는 역할을 수행하며, 통신방법에 대한 모듈을 플러그인 형태로 추가 및 제거가 가능하도록 구성이 되어 있다. 또한, 기계와 사용자간에 기본적인 환경설정을 위한 사용자 인터페이스를 WEB 2.0기반에 AJAX기술을 통해 제공한다.

2.2 도메인 관리모듈

Event Engine 및 LOG Engine, Repository는 이동 단말 및 서비스 서버, 센서 등에서 발생되는 비표준/표준형식 데이터를 UCMF로 변환 및 UCMF형식의 정리된 데이터를 기반으로 Log Engine을 통해 기록과 더불어 Event Engine을 통

한 이벤트화를 통해 보안관련 정보를 추출/생성 및 통보 등의 역할을 수행한다. 또한 관리자 도구로부터 전달받은 정책을 해당 이동단말이나 센서, 서비스 장비, 네트워크 장비 등에 맞는 Rule 형식으로 변환[3-4]하여 적용하고 적용내용과 적용과정 모니터링 내용을 로그 및 이벤트형태로 기록과 함께 문제점 및 처리결과 등을 종합적으로 통보하는 역할도 수행한다.

2.3 분산처리 엔진모듈

u-Ware 시스템 간에 효율적인 분산처리를 담당하는 엔진으로써 해당 u-Ware 시스템이 과부하나 시스템 점검, 시스템 중지, 시스템 재시작 등의 다양한 문제 발생 시에 인접한 u-Ware 시스템 간에 동적으로 분산처리를 수행할 수 있도록 기능을 제공한다.

2.4 인증/위임 처리모듈

Security Policy Manager와 Authentication Manager로 구성이 되어 있으며 Security Policy Manager를 통해 정책기반에 사용자, 이동단말, 서비스, 서비스 제공서버 등의 다양한 객체를 추가/등록/삭제/인가 등의 다양한 관리를 수행하며, Authentication Manager를 통해서 이동단말과 사용자에 대한 인증/위임처리를 담당한다. 또한, 인증/위임 모듈의 경우 플러그인 기술을 통하여 자체적으로 개발한 인증/위임 시스템을 적용하거나 공인된 인증시스템과 연동이 가능하다.

2.5 캐싱 모듈

메모리 데이터베이스를 이용하여 u-Ware 시스템의 내부의 모듈 간에 데이터를 전송하고 분석, 생성, 추출 등의 처리를 수행하는데 있어서 체계적인 관리와 대량의 데이터를 안전하면서 고속으로 처리하기 위한 부분이다.

2.6 위치정보 관리서버 모듈

각 u-Ware 시스템과 연결된 시스템들 간에 위치 확인을 위한 관리서버 모듈로써 외부 LBS (Location Based Service)나 GPS(Global Positioning System)서버등과의 연동을 통하여 이동단말 및 각종 센서, 임베디드 장치, 서비스 제공 서버들의 위치파악과 더불어 동일도메인 내의 u-Ware 시스템들의 위치를 파악하는 역할을 수행하는 서버 시스템이다.

2.7 관리자 도구

u-Ware 시스템을 관리하며 다양한 장치에 대해 작성/설정/관리와 더불어 수집되고 통보되어진 데이터에 대한 분석 및 관리, 시각화된 인터페이스를 통한 종합적인 관제가 가능하도록 기능을 제공하는 관리 시스템이다.

3. 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.

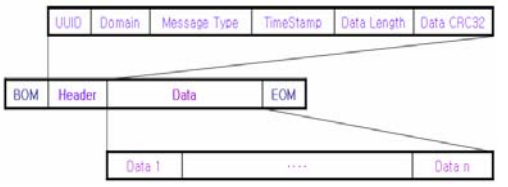

그림 2. UCMF 구조
Fig 2. UCMF Structure

전체적인 구조는 메시지의 시작을 나타내는 BOM 필드, 메시지의 끝을 나타내는 EOM 필드와 메시지 정보를 담고 있는 헤더 필드, 관련 데이터가 담겨 있는 데이터 필드 이렇게 4가지 부분으로 나뉜다. 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 1. 메시지 종류
Table 1. Message Type

종류	설명
N	일반 메시지
S	시스템 메시지 (ALIVE, PING/PONG 등)
M	모니터링 메시지
C	제어 메시지
1-9	우선순위 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 전송되어진다.

4. 처리 단계

문제 발생 시나 수집된 데이터에 대해 세부적으로 5단계의 처리를 거쳐 분석 및 처리 후 통보된다.

4.1. 수집 및 기록

u-Ware와 연결된 정적인 장비 및 센서, 이동단말, 서비스 제공 시스템등간에 주고받는 모든 데이터를 수집하고 기록하는 하는 단계로 전체 시스템 구성 요소 중 입력부분에 해당한다.

4.2 문제발생 인지

실시간 모니터링을 통하여 해킹이나 악의적인 코드, 바이러스 등을 탐지하는 단계이다. 이 단계에서는 탐지된 이상 트래픽이 이미 구축되어 있는 문제점 데이터베이스와 비교하며, 신규 문제점인지 이미 알려진 문제점인지에 대해 얼마만큼 빨리 파악하는가가 중요하다.

4.3 문제점 분류 및 분석

탐지된 문제점을 이벤트화와 더불어 문제점의 종류 및 중요도를 분석하는 단계로 이벤트화 즉시, 필터링 룰에 의해 필터링된 이벤트는 데이터베이스에 기록을 지며, 문제점의 분류 및 위험의 영향도를 종합적으로 판단하는 것이 중요하다.

4.4 경보 및 관리

이벤트를 관리자 도구로 통보와 더불어 미리 정의된 정책에 따라 대응을 하는 단계이며, 대응은 자체적인 학습에 의한 방법과 기존에 관리자 도구를 통하여 설정되어진 정책기반에 대응으로 나뉜다. 또한, 경보단계는 국가사이버 안전센터의 사이버위기 경보단계를 기준으로 통보되어 진다 [6].

4.5. 정리

사전에 정의된 문제에 따른 조치 방법에 따라 처리단계를 재이행 및 문제에 대한 리포팅, 이벤트 분석, 해당 문제점에 대한 보호대책을 수행하는 단계이다.

이러한 과정을 통해 웜이나 바이러스, 해킹의 불법적인 접속과 더불어 서비스 제공 등으로 인하여 발생되는 대량의 데이터를 처리하여 보안 관리의 기본이 되는 로그와 이벤트 데이터를 생성 및 기록, 통보하게 된다.

Ⅳ. 구현

본 프로토타입 u-Ware 시스템은 Windows XP 및 Windows XP Embedded Edition 기반에서 개발 및 동작한다. 시스템은 크게 도메인서버와 위치정보 관리서버, 관리자 도구로 이렇게 3가지로 구분된다. 이러한 각 부분들은 하나의 임베디드 시스템에 모두 탑재될 수 있으며,각각 별도 분리운영이 가능하도록 구성되어 있다.

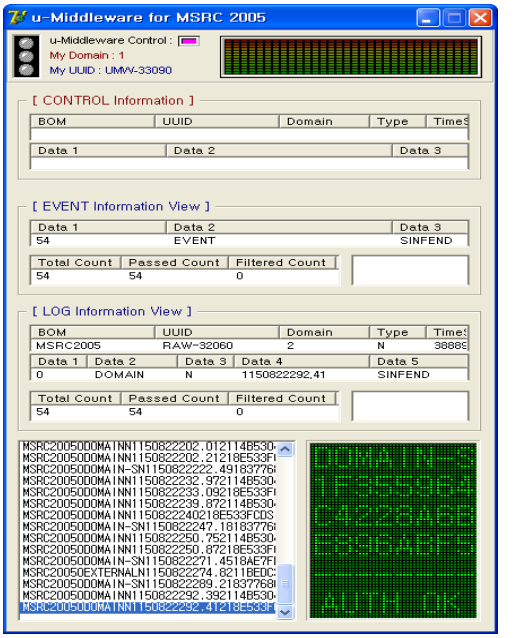

그림 3. 도메인서버
Fig. Domain Server

1. 도메인 서버

현재 유비쿼터스 환경을 위하여 상용화된 각종 센서를 비롯하여 장비들은 표준화된 데이터 형식보다는 제조사 자체의 형식으로 데이터를 전송하

는 구조를 가지고 있다. 이에 도메인 서버는 컴포넌트 관리모듈, 도메인 관리모듈, 인증/위임 처리모듈, 캐싱모듈, 분산처리 엔진모듈로 구성된 시스템으로써 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.

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 나뉜다. 자체적인 학습에 의한 처리 부분은 플러그인 기능을 이용하여 원하는 시점에서 원하는 학습방법을 통한 필터링 정보를 적용할 수 있다.

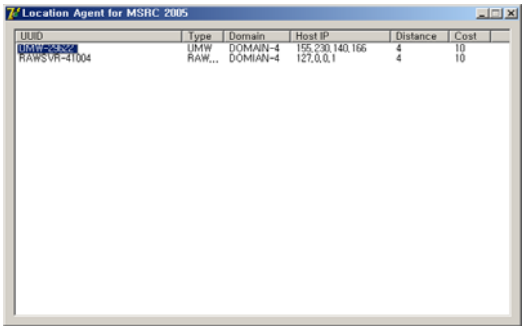

그림 4. 위치정보 관리서버

Fig 4. Location Information Management Server

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.

3. 통합 보안관리 도구

통합 보안 관리를 위한 도구로써 정책과 필터링 정보를 제외한 나머지 정보는 그림 5와 같이 시각적으로 표현하여 종합적인 상황을 한눈에 파악함으로써 보안관리 효율을 높이도록 구성되어 있다.

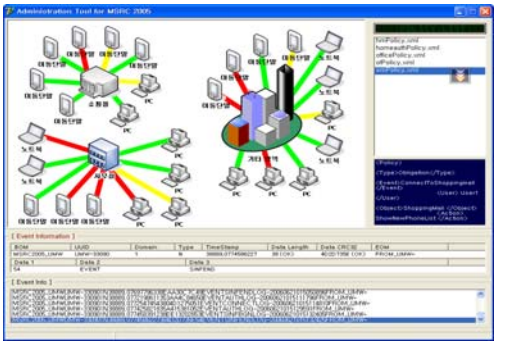

그림 5. 통합 보안관리 도구

Fig 5. Total Security Management Tools

또한, 도구에서 처리할 수 있는 일은 다음과 같다.

- 정책 작성 및 조회/관리
- 필터링 정보 설정 및 조회/관리
- 위치정보 관리서버에 등록된 시스템의 위치 확인
- 연결된 시스템과 이동단말, 사용자 상태 모니터링

시각화 기능은 보안 관리를 함에 있어서 얼마만큼 빠르게 문제발생 여부를 관리자가 인지하고 대응을 하느냐가 관건이므로 이에 대해 가장 직관적이고 원색을 사용하여 빠르게 인지하는데 초점을 맞추었으며, 도메인서버에서 전달받은 EVENT 정보에 대해 분석을 수행하며 분석된 내용을 다양한 형태로 도표 및 그래프, 히스토리, 목록 등의 다양한 형태의 리포팅 기능을 통하여 단기적인 부분에서부터 장기적 부분까지 팀 단위 및 그룹단위의 보안관리 문제점을 파악하고 대응할 수 있도록 구성되어 있다.

Ⅴ. 결론

본 논문에서 제안한 프로토타입 u-Ware 시스템은 유비쿼터스 환경에서 서비스 제공 시스템과 네트워크 장치, 이동단말, 임베디드 장치에서 발생할 수 있는 각종 상황과 이에 따른 보안관리, 생성되는 데이터 등을 통합 관리할 수 있는 시스템이다. 모든 시스템은 임베디드화가 가능하도록 구성되어 적시 적소에 활용이 가능하므로 여러 개의 도메인에서 운영이 가능하며, 인접한 u-Ware 시스템들간에 연동하여 통합 관리가 가능하므로 실제 환경에서 발생할 수 있는 다양한 문제점에 효율적으로 대처할 수 있도록 구성하였다. 또한 추후 인접 u-Ware 시스템 간에 동적 분산 처리를 통해 대량의 데이터를 처리하며, 수집/분석 과정에서 조기경보 기능을 구축하여 사후처리가 아닌 사전탐지 기능을 통해 보다 효율적인 보안 관리를 수행할 수 있도록 할 것이며, 스스로 학습에 의한 최적화된 보안 관리를 할 수 있는 방안에 대하여 추가적으로 연구와 더불어 대량의 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," Proceedings of 18th Annual Computer Security Applications Conference, pp 249-260, 2002.

[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, Mustaque Ahamad, "Generalized role-based access control for securing future applications," In Proceedings of the 23rd National Information Systems Security Conference(NISSC), pp.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.

[5] F. Stajano, "Security for Ubiquitous Computing," first Security & Privacy supplement to IEEE Computer, April 2002.

[6] 국가사이버안전센터, "사이버 위기경보 체계", http://ncsc.go.kr/.

[7] 권기훈, 한영구, 정석봉, 김세헌, 이수형, 나중찬, "트래픽 분석에 의한 광대역 네트워크 조기경보 기법", 한국정보보호학회지, 제14권 제4호, pp.111-121, 2004. 8.

[8] 정재훈, 이승윤, 김용진, "인터넷 트래픽 수동적 측정 도구 Cflowd의 설치 및 설정 방법 (for Linux 2.4.5)", IPv6 포럼 코리아 기술문서 TM2001-006, 2001.

[9] R. Jain and S. Routhier, "Packet Trains-Measurements and a New Model for Computer Network Traffic," IEEE Journal of Selected Areas in Communications, Vol. SAC-4, No. 6, pp.986-995, September 1986.

[10] NetFlow, http://www.cisco.com/warp/public /cc /pdiosw/ioft/netlct/tech/napps_wp.htm

[11] 이글루시큐리티, "SPiDER-TM", http://www .igloosec.co.kr/.

저 자 소 개

배 현 철

2003년 동명정보대학교 정보통신공학 학사

2005년 경북대학교 정보보호학과 석사

2005년~현재 경북대학교 컴퓨터과학과 박사과정, 관심분야 : 임베디드 소프트웨어, 분산 처리, 모바일 서비스, 웹서비스, 보안 관제, 조기 경보, 데이터 시각화

Email: swkim@woorisol.knu.ac.kr

김 상 욱

1979년 경북대학교 컴퓨터공학 학사

1981년 서울대학교 컴퓨터과학과 석사

1989년 서울대학교 컴퓨터과학과 박사

1988년~현재 경북대학교 전자전기컴퓨터학부 교수, 관심분야 : 모바일 멀티미디어 컴퓨팅, 멀티미디어 컨텐츠 저작 및 인간과 컴퓨터의 상호작용, DMB 시스템

Email: swkim@cs.knu.ac.kr