情 報 保 護 學 會 誌
第19卷 第2號, 2009. 4

유비쿼터스 환경의 모바일 단말 보안 관리 기술 개발

김 상 욱*

요 약

본 연구는 여러 위치에서 이동 중인 다양한 유형의 단말기에 대해 보안을 관리하는 통합 시스템을 개발하는 것이다. 이 기술은 모바일 단말 인증, 모바일 단말 신뢰, 개인 프라이버시 보호, 3차원 시각화 기술에 의한 모바일 단말 보안 관리 기술이다. 인증과 신뢰 기술은 다른 도메인에 접근하더라도 신뢰할 수 있는지를 검사한다. 개인 프라이버시 보호 기술은 접근 기록을 사용자가 관리하는 기술이다. 3차원 시각화 기술은 단말의 이동과 접근을 3차원으로 모니터링한다. 이러한 모바일 단말 보안 관리 기술은 여러 기술을 파생하거나 파급할 수 있는 중요한 기술이다.

Ⅰ. 서 론

유비쿼터스 환경에서의 모바일 단말 보안 관리 기술은 보안 정책에 따라 모바일 단말기의 이동과 행위에 대한 보안 관리를 수행하는 기술이다.

이전 보안 관리 기술은 도메인마다 따로 관리하기 때문에 다양한 객체, 다양한 모바일 기기, 다양한 모바일 서비스 상호 간의 보안 관리가 어려웠다[1,2,8,9].

또한, 관리적 측면에서도 모바일 단말의 현재 상황 정보가 자주 변하기 때문에 보안 정책의 설정, 관리, 접근 제어에 어려움이 있다.

그러므로 유비쿼터스 환경에서는 다양한 모바일 단말의 빈번한 이동으로 발생하는 보안 취약점을 관리하는 기술이 필요하다.

이 통합 관리 기술은 유비쿼터스 환경에서 모바일 단말을 신뢰할 수 있는지를 알아내고, 빈번한 이동에 의한 사용자의 프라이버시를 보호하는 것이 핵심이다. 그 외에도 단말에 의하여 정보 엑세스를 모니터링하는 3차원 시각화 기술도 포함한다.

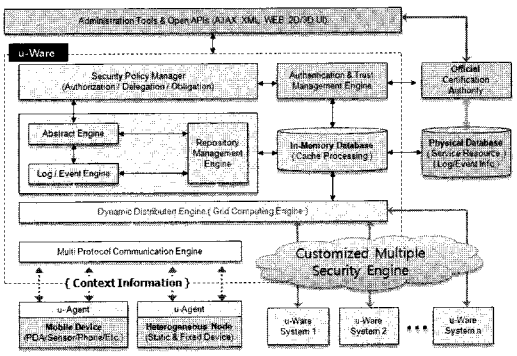
이 기술은 모바일 단말에 대한 보안 관리는 물론 디지털 기기의 유선 네트워크 이용에도 적용할 수 있다. 또한 다양한 형태의 분산 이동 시스템에도 적용할 수 있다.

이 글은 제 II절에서 모바일 단말 보안관리 시스템 구조를 설명한다. 제 III절과 제 IV절에서는 모바일 단말 신뢰 기술과 프라이버시 관리 기술을 설명한다. 또 제V절에서는 모바일 단말 모니터링과 3차원 시각화 기술을 설명한다. 제 VI절에서는 이러한 보안 기술을 적용한 응용 기술을 보인다.

Ⅱ. 모바일 단말 보안 관리 시스템 구조

이 절에서는 서비스를 요구하는 모바일 단말과 보안 서비스를 제공하는 서버에서의 모바일 단말 보안 관리 시스템 구조를 설명한다. [그림 1]은 세 계층의 구조로 구성되는 모바일 단말 보안 관리 시스템이다.

이 시스템에는 여러 관리부, 저장소, 각 에이전트가 있다.



〔그림 1〕 모바일 단말 보안 관리 시스템 구조

* 경북대학교 전자전기컴퓨터학부 (kimsw@knu.ac.kr)

- 통합 컴포넌트 관리부: 모바일 단말과 통신을 관리한다. 또한 코바의 객체 요구 매개자 구조와 오브젝트 네이밍 서비스를 사용하여 모바일 단말과 자원을 관리한다.
- 컨텍스트 관리부: 모바일 단말의 현재 상황 정보를 수집하고 관리한다.
- 이벤트 관리부: 모바일 단말 보안 관리 시스템에서 일어나는 모든 작업에 대한 정보를 저장한다.
- 저장소: 서버 내 다양한 자원이나 서비스에 대한 일괄적인 표현 및 상태에 대한 정보를 제공한다.
- 보안정책 관리부: 모바일 단말에 대한 보안정책을 설정하여 데이터베이스화한다. 컨텍스트 관리부에서 받은 정보와 보안정책의 일치 여부에 따라 모바일 단말이 요구한 서비스의 실행 여부를 결정한다.
- 인증 관리부: 모바일 단말에 대한 인증을 수행한다.

이 모바일 단말 보안 관리 시스템은 아래와 같이 동작한다. 먼저 모바일 단말은 도메인에 있는 자원 접근을 요청하는 메시지를 전송한다. 이를 위해 서버는 작업 정보를 저장한 후 모바일 단말에 대해 평판과 과거 사용자의 사용 내역을 조사하여 자원에 대한 인증 여부를 판단한다. 인증 후 다양한 센서를 통해 모바일 단말의 상황 정보를 수집하여 저장하고 이를 통해 접근하려는 객체 및 수행 액션 정보를 추출한다. 모바일 단말이 정책 데이터베이스에 저장되어 있는 보안 정책에 벗어나는 행동을 하지 않는지에 대해 룰 베이스 필터링을 통해 검사하며 이로써 도메인에 대한 모바일 단말의 보안 서비스를 제공한다.

정책 데이터베이스에는 인가정책, 위임정책, 의무정책이 있다. 인가정책은 접근 제어를 위한 정책으로 모바일 단말의 도메인 내 장치나 자원에 대한 접근 요청에 대해 수행 여부를 결정한다. 위임정책은 특정 상황에서의 권한에 대한 위임을 표시하는 신뢰 관리 정책이다. 의무정책은 이벤트-조건-동작 패러다임의 정책이다. 즉, 객체와 컨텍스트 관리부로부터 받은 상태정보를 이벤트로 추출하여 동적으로 실행하는 정책이다.

주체는 사용자 모바일 단말이며 객체는 주체가 동작을 수행하려는 목적 장치나 서비스 객체이다. 컨텍스트는 장소, 시간과 같은 주체가 처한 상황 정보이며 허용 여부는 동작의 수행 여부를 나타낸다.

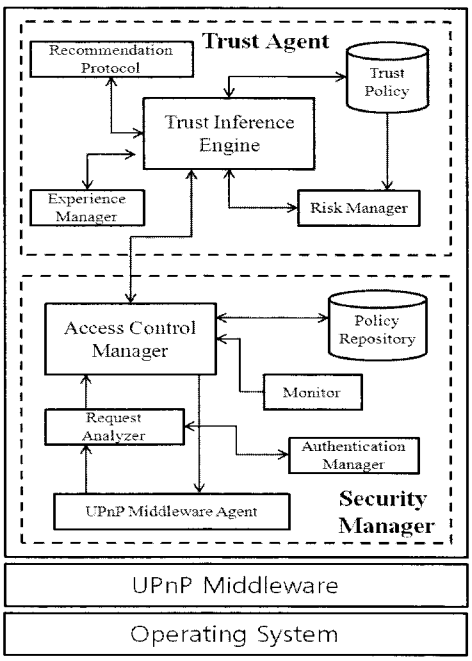
Ⅲ. 모바일 단말 신뢰 관리 기술

이 절에서는 모바일 단말이 이동 중에 어떤 자원에 엑세스하려 할 때, 모바일 단말기가 신뢰할 수 있는 단말기인지 아니지를 알아내고 관리하는 기술을 설명한다. 신뢰를 관리하는 모듈 구조와 모듈의 신뢰 관리 동작을 설명한다.

3.1 신뢰 관리 모듈

[그림 2]는 모바일 단말의 신뢰 관리 모듈이다. 모든 단말 장치를 연결하여 상호작용을 수행하는 UPnP 미들웨어에 보안 관리자와 신뢰 관리 에이전트 모듈이 상호 연동한다. 이 신뢰 관리 모듈에는 다음의 관리자가 있다.

- 경험 관리자: 모바일 단말 사용자와 서비스 도메인 서버 사이의 상호작용 경험을 통해 신뢰 값을 계산한다.
- 위험 관리자: 모바일 단말 사용자의 접근에 의한 위험을 줄인다.
- 추천 관리자: 타 신뢰 도메인 서버와의 사이에서 신뢰 정보를 교환한다.

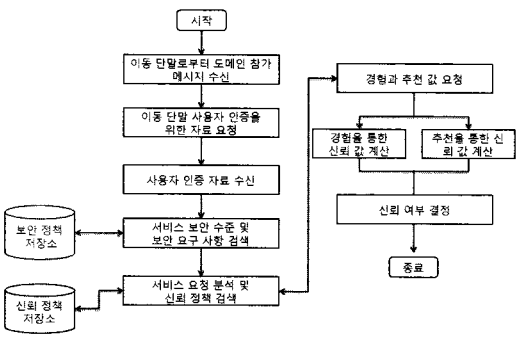


[그림 2] 모바일 단말의 신뢰 관리 모듈

- 신리 정책 저장소: 신뢰 정책을 저장한다.
- 신뢰 추론 엔진: 모바일 단말 사용자에 대한 최종 신뢰 여부를 판단한다.

어떤 모바일 단말이 특정 자원에 접속하여 서비스를 요구하면 이 단말에 대한 인증과 신뢰성을 검사한다.

[그림 3]은 신뢰 관리 모듈이 모바일 단말에 대한 신뢰 관리를 수행하는 과정이다. 모바일 단말이 서비스 도메인에 들어오면 멀티캐스팅으로 도메인 참가를 알린다. 서버는 이를 수신한 후 모바일 단말에게 사용자 인증을 위한 자료를 요청한다. 서버가 인증 자료를 수신하면 사용자에 대한 인증을 위해 서비스 도메인의 보안 정책 저장소를 검색하여 서비스의 보안 수준 및 보안 요구사항을 검색한다. 그리고 이전의 서버에게 해당 사용자에 대한 경험과 추천을 요청한다. 다른 서버로부터 경험과 추천을 수신 후 신뢰 추론 엔진이 먼저 신뢰 정책 저장소에 있는 사용자에 대한 신뢰 정책을 검색하고, 신뢰 정책에 명시된 경험과 추론이 신뢰 값에 주는 가중치에 의하여 경험 관리자와 추천 관리자에 신뢰 값을 요청한다. 경험 관리자에서 경험을 통한 신뢰 값을 계산하고 추천 관리자에서 추천을 통한 신뢰 값을 계산한 뒤 이들 계산 값들에 가중치를 주어 최종 신뢰 값을 계산하고 위험 관리자에서 서비스 접근에 필요한 보안요구 사항 만족여부를 판단한 뒤 신뢰 추론 엔진에서 최종 신뢰 여부를 결정한다.



〔그림 3〕 신뢰 관리 수행

3.2 경험을 통한 신뢰 값 계산

경험은 모바일 단말 사용자와 서비스 도메인 서버 사이에서 행동한 결과이다. 경험관리자는 사용자와 서버 사이의 상호작용 결과를 바탕으로 아래와 같이 신뢰 값을 계산한다[3,4].

$$VA_j = \max\{(A_j \times 2^C)/j \times (S_j/TS), -1\}$$
$$EV_i = EV_{i-1} \times (1-|B \times VA_j|) + B \times VA_j$$

여기에서 A_j는 j 번째 액션으로 긍정적인 액션이면 +1이고, 부정적인 액션이면 -1이다. C는 연속으로 부정적인 액션을 수행한 횟수이다. S_j는 j 번째 액션이 접근했던 서비스 보안 수준이다. TS는 서비스 도메인에서 정의한 최상위 보안 수준이다. VA_j는 j번째 액션 값이다. EV_i는 i번째 신뢰 값이고 B는 새로운 액션 값에 대한 가중치이다. EV_{i-1}은 i-1번째 신뢰 값이다.

이 수식에 따르면 상호작용은 결과에 따라서 긍정적인 액션과 부정적인 액션으로 나눌 수 있다. 사용자와 서버의 상호작용 외에도 서비스 보안 수준에 따라 연산이 달라진다. 즉, 서비스 도메인에서 제공하는 서비스는 총[1, TS] 등급으로 나눠지고, TS는 최상급의 보안 수준을 나타낸다. 각각의 서비스는 관리자가 미리 정의해 놓은 서비스 보안 수준(S)을 가지고 있다. 예를 들어 보안 수준이 1인 서비스에 행한 부정적인 행위와 보안 수준이 3인 객체에 행한 부정적인 액션이 경험 값에 주는 영향은 경험을 통한 신뢰 값을 계산할 때 다르게 반영한다. 또한, 연속으로 부정적인 액션이 발생하면 신뢰 값은 떨어진다. 그러므로 이를 반영하기 위하여 연속으로 부정적인 액션이 두 번 발생하는 경우에는 C=1로 설정되면서 처음 부정적인 액션보다 신뢰성이 더 떨어진다.

결국, 특정 기간 동안 j번째 액션이 가지는 값을 VA_j라 하고 i개 액션이 발생한 후의 신뢰 값을 EV_i라고 하며, 그 전에 계산했던 신뢰 값과 가장 최근에 발생했던 신뢰 값에 가중치 B를 두어 경험을 통한 신뢰 값을 계산한다.

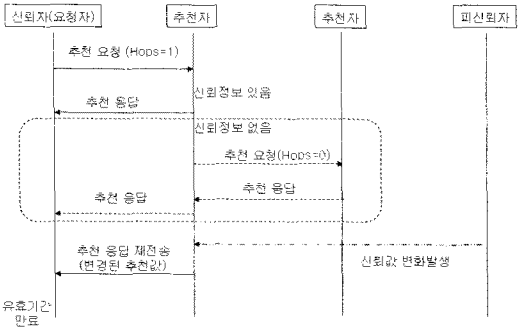
3.3 추천을 통한 신뢰 값 계산

추천이란 사용자가 특정 도메인의 서비스를 이용한 정보가 없거나 부족할 경우에는 현재의 서버가 특정 신뢰 값 이상을 가진 추천자(서버)에게 사용자에 대한 신뢰 값을 요청하는 것이다. 추천받은 이 신뢰 값을 이용하여 현재의 모바일 단말의 신뢰 값을 계산하는데 사용한다.

이때 현 도메인 서버를 요청자로 하여 특정 신뢰 값 이상인 추천자들에게 추천 프로토콜로 사용자에 대한 신뢰정보를 요청한다[4,5,6].

추천 요청 메시지는 요청메시지 아이디, 요청자 아이디, 피신뢰자 사용자, 추천자 아이디, 추천 메시지의 유효기간, 메시지가 전달되는 도메인의 홉으로 구성된다. 홉은 추천 요청 메시지가 전파되는 한계를 명시한 것으로, 추천자가 대상자에 대한 정보가 없는 경우에 다른 추천자에게 추천 메시지를 보내는 단계이다. 추천자에게 대상자에 대한 신뢰정보가 있을 때는 홉스를 설정해도 사용하지 않는다. 예를 들어, 신뢰정보가 없을 때는 홉스를 1로 설정하면 추천자는 자기가 신뢰하는 다른 추천자 1인에게 요청 메시지를 전송하고, 홉스를 0으로 설정하면 더 이상 다른 추천자에게 요청 메시지를 전송하지 않는다.

또한 요청에 대한 응답 메시지는 요청메시지 아이디, 추천자 아이디, 추천하는 신뢰 값, 메시지 전송 시간(타임스탬프)로 구성한다. [그림 4]는 추천 프로토콜의 메시지 흐름이다.



〔그림 4〕 신뢰 관리 추천 프로토콜

신뢰요청자가 특정 신뢰 값 이상의 추천자에게 피신뢰자에 대한 추천 요청 메시지를 전송한다. 요청 메시지를 전송할 때 홉스를 1로 가정한다. 추천자가 피신뢰자에 대한 신뢰 값을 가지고 있으면 추천 응답 메시지에 추천하는 신뢰 값을 넣어서 신뢰자로 전송하고 홉스 값은 무시한다. 만약 추천자가 신뢰 값을 갖고 있지 않고 홉스가 0이 아니면, 자신이 신뢰하는 다른 추천자에게 Requester_ID를 자신으로 변경한다. 또한, 홉스를 1 감소하며 유효기간도 1/2로 감소하여 추천 요청 메시지를 전송한다. 추천자를 경유할 때마다 홉스를 1씩 감소하여 0이 되면 요청 메시지를 수신한 추천자는 다른 추천자에게 더 이상 요청 메시지를 전송하지 않는다. 피신뢰자에 대한 신뢰 값을 가지고 있으면 추천 응답 메시지에 신뢰 값을 넣어서 추천자에게 전송한다.

추천자가 피신뢰자에 대한 신뢰 값을 신뢰요청자에게 전송한 뒤 상호작용으로 피신뢰자의 추천자에 대한 신뢰 값이 변경 되었으며, 추천 요청 메시지의 유효기간이 만료되지 않았으면 타임스탬프를 현재 전송 시간으로 설정하고 변경한 신뢰 값을 추천 응답 메시지에 넣어 재전송한다.

3.4 최종 신뢰 값 계산

위에서 경험을 통해 얻은 신뢰 값(EV)과 추천을 통해 얻은 최종 추천 값(RV)에 가중치 wi 를 주어 서비스 사용자에 대한 최종 신뢰 값을 아래와 같이 계산한다.

$$TV = EV \times w_1 + RV \times w_2$$
$$w_1 + w_2 = 1$$

여기에서 $0 \leq w_i \leq 1$이다. 도메인 내에 등록된 사용자에게는 경험에 가중치를 높게 주고, 처음 들어온 사용자에게는 추천에 보다 높은 가중치를 준다. 일반적인 경우에는 w_1과 w_2의 비율을 6 : 4로 하며, 계산 결과가 도메인에서 요구하는 신뢰 값을 넘은 경우에는 모바일 단말에게 서비스를 허용한다.

3.5 위험 관리

위험 관리는 신뢰 관리 시스템에서 보안상 위험을 줄인다[5,6]. 다양한 모바일 단말이 서비스에 접근할 때 신뢰가 있더라도 접근하려는 서비스나 자원의 보안 요구사항을 만족하지 못하면 위험으로 간주하고 '위험' 신호를 신뢰 추론 엔진에 전달한다.

Ⅳ. 모바일 단말 프라이버시 관리 기술

유비쿼터스 환경에서 사용자는 이동이 자유롭고 여러 도메인에서 제공하는 서비스를 편하게 이용하기를 원한다. 이 과정에서 사용자는 자신의 개인 정보를 서비스 제공자에게 제공하거나 여러 곳에 기록을 남긴다[8].

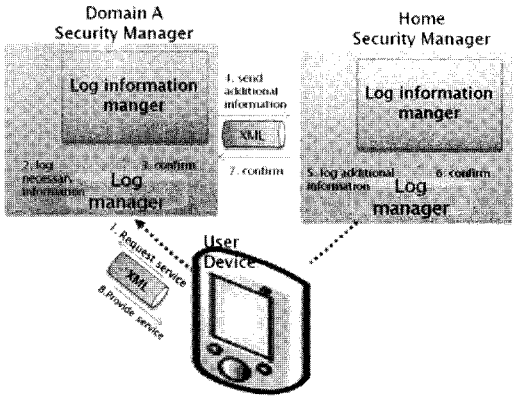
모바일 단말 프라이버스 관리 기술은 개인 정보를 서비스 제공자가 관리하는 것이 아니라 사용자가 직접 관리하면서 보호하는 기술이다. 즉, 모바일 단말 사용자는 자신의 정보가 누가 언제 어떻게 사용하는지에 대한 자기 제어권을 가지도록 한다. 이러한 연구는 여러 곳에서 진행 중이지만 유비쿼터스 환경과 모바일 단말에 대한 연구는 매우 미흡하다[8,9,10,11].

4.1 개인 로그 관리 시스템 구조

개인 정보를 보호하기 위한 개인 로그 관리 시스템 구조는 [그림 5]와 같다. 모바일 단말이 서비스 제공자에게 서비스를 요청하면 이때 모바일 단말 사용자를 인증한다.

이 인증은 앞 절의 모바일 단말 보안 관리 시스템에 의해 인증한다. 즉, 도메인간을 이동할 때 홈 도메인의 인증 서버를 통하여 자신의 인증 정보를 전달한다. 홈 시스템과 다른 도메인의 시스템은 모두 신뢰기관으로부터 인증된 상태인 제 3기관을 통한 신뢰 시스템이다.

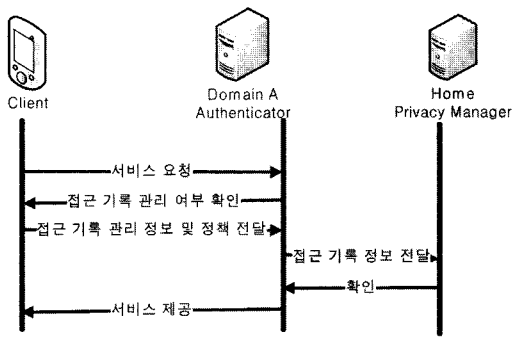
접근에 대한 인증이 끝나면 서비스를 요청한다. 서비스 제공자는 해당 요청에 따라서 서비스를 제공하기 전에 사용자가 직접 전근 기록 정보를 관리하는지 확인한다. 사용자는 자신의 접근 기록 정책을 서비스에 맞게 전달한다. 서비스 제공자는 전달받은 정보를 바탕으로 자신의 서비스에 맞게 협상을 한 후 사용자 홈 도메인 관리자에게 접근 기록 정보를 전달한다. 그런 후 사용자에게 서비스를 제공한다.



[그림 5] 개인 로그 관리 시스템

4.2 접근 정보 전달 기법

[그림 6]은 접근 정보를 사용자 홈 도메인으로 전달하는 과정이다. 사용자는 이동하면서 이동한 도메인에 서비스를 요청한다. 서비스 제공자는 접근 기록 정보를 사용자가 관리하는지에 대해 사용자에게 확인한다. 사용자는 접근 기록 정보를 전달할 수 있는 홈 도메인 서버의 URI와 접근 기록 정보에 대한 사용자의 정책을 전달한다. 서비스 제공자는 해당 정책과 서비스 제공자의 접근 기록 정보 사이에서 협상을 통해서 전달할 정보를 결정한다. 홈 도메인 서버로 접근 기록 정보를 전달한 후 사용자가 요청한 서비스를 제공한다. 서비스 제공자는 자신의 접근 기록 정보를 저장할 때 사용자를 식별할 수 있는 코드, 과금 정보, 추후 서비스 내역의 추적을 위한 서비스 제공에 대한 해쉬 코드를 포함한다. 이러한 정보들은 최소화한다. 이 외의 정보들에 대해서는 사용자가 관리할 수 있도록 홈 도메인 서버로 전달한다.



[그림 6] 접근 정보 전달

사용자가 관리하는 접근 정보를 요청하면 서비스 제공자는 홈 도메인 서버의 URI로 해당 서비스에 대한 해쉬 코드를 보낸다. 홈 도메인 서버는 사용자가 정의한 정책에 따라서 해당 정보를 전달할 것인가를 결정한다. 이때 등급에 따라 어느 정도의 정보를 전달할 것인가를 개인 제어 하에서 전달한다. 만약에 정책이 결정되어 있지 않으면 미결정 정책에 대해서 사용자가 직접 검사할 수 있다.

정책은 서비스와 클래스에 따라 나뉜다. 접근 기록 정보는 각 서비스에 따라 형태도 다르고 저장해야 하는 정보도 다르다. 따라서 서비스에 따라 해당 서비스에 맞

는 서비스 관리 정책을 지정한다. 혹은 전체 클래스에 따른 정책 결정으로 시간, 콘텐트 내역 등 에 따른 정책을 지정한다.

4.3 접근 기록 정보 전달과 요청 프로토콜

접근 기록을 전달하려면 도메인의 정보와 정책을 전달하고 해당 정책에 따른 접근 기록 정보를 전달하는 메시지가 필요하다. 서비스를 요청하면 서비스 제공자는 사용자의 도메인에게 자신의 서비스명을 포함하여 사용자의 정책 전달을 요청한다. [그림 7]은 사용자 정책을 전달하는 메시지이다.

```
<?xml version="1.0" encoding="utf-8"?>
<Client>
  <HomeServer>155.230.118.69</HomeServer>
  <AuthCode>4302c7ee32602c88d91a3d5..</AuthCode>
  <ExpireDate>2007-12-31 23:59:59</ExpireDate>
  <Audio_Information>allow</Audio_Information>
  <ContentInformation>deny</ContentInformation>
</Client>
```

〔그림 7〕 사용자 정책 전달 메시지

도메인 서버는 서비스명을 확인하여 해당 서비스에 대한 특정 정책을 가지고 있으면 해당 정책을 전송하고, 그렇지 않으면 클래스 관련 정책을 전송한다. 클래스 관련 정책으로는 비디오, 오디오, 콘텐츠와 같이 구성된 정책이다. 전송하는 메시지에는 도메인 서버 주소와 인증 코드, 이 정책 메시지의 유효 기간, 정책들을 정의한다. [그림 8]은 서비스 제공자가 정책에 따라 협상한 후 접근 기록을 전달하는 메시지이다.

```
<?xml version="1.0" encoding="utf-8"?>
<Client>
  <AuthCode>4302c7ee32602c88d91a3d5..</AuthCode>
  <HashCode> c3557ca22ada1ccafcc...</HashCode>
  <ContentInformation>
    < RawData > Adding content disposition header:
Content-Disposition: attachment; filename="28wlts-
sample.avi" </RawData>
  </ContentInformation>
</Client>
```

〔그림 8〕 접근 기록 정보 전달 메시지

접근 기록 전달 메시지에는 인증 코드와 해당 기록에 대한 유일성을 구분하는 유니크 코드이며 시간, 콘텐트 ID를 포함하여 생성한 해쉬 코드를 삽입한다. 협상에 따라서 XML 형태로 접근 기록 정보를 바꾸어 전달한다.

사용자가 정의한 정책과 서비스 제공자가 정의하는 접근 기록 정보에 따라 전달 데이터를 협상한다. 만약 서비스에 대한 사용자 정책이 존재하면 그 정책에 따라 정보를 전달한다. 만약 서비스에 대한 정책이 정의되어 있지 않으면 클래스에 대한 정책을 통해서 서비스가 제공하는 접근 정보와 비교하여 전달할 정보를 결정한다. 그즉, 서비스 제공자가 제공하는 정보의 종류에 따라 사용자의 정책과 비교하여 접근 정보에 대한 정책을 결정한다.

사용자에게 기록된 접근 기록 정보가 요구될 수도 있다. 서비스 제공자가 개인화된 서비스를 제공하거나 적법한 절차에 따라서 공적인 요구에 의해 개인의 접근 기록을 요청하는 경우가 발생한다. 이 경우 서비스 제공자는 자신이 가지고 있는 해쉬 정보를 사용자의 도메인 서버에 보내어 해당 정보를 요청 할 수 있다. 요청 받은 접근 정보에 대해서 정책을 확인하고 전송 가능한 정책이면 전송한다. 만약 해당 정책이 정의되어 있지 않으면 사용자의 결정을 요청하고 피드백 받아서 결정한다.

```
<?xml version="1.0" encoding="utf-8"?>
<Client>
  <AuthCode>4302c7ee32602c88d91a3d5..</AuthCode>
  <HashCode> c3557ca22ada1ccafcc...</HashCode>
</Client>
```

〔그림 9〕 접근 정보 요청 메시지

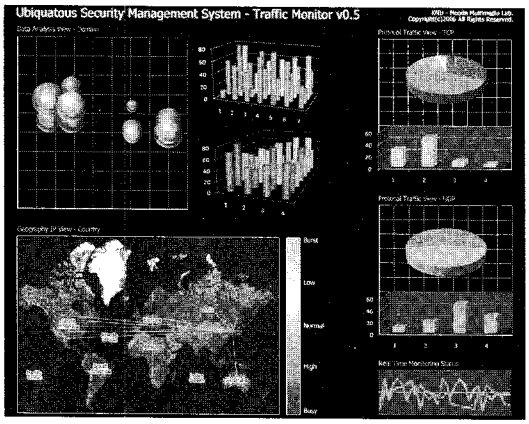
이 프라이버시 관리 기술은 개인 정보를 열람하려면 개인의 동의가 있어야 하므로 개인 정보의 무분별한 유출을 막을 수 있다. 또한 권리가 있는 서비스 제공자는 기존 프라이버시 관리 기술과 사용상의 차이 없이 편리한 서비스를 제공할 수 있다.

V. 모바일 단말 모니터링과 3차원 시각화 기술

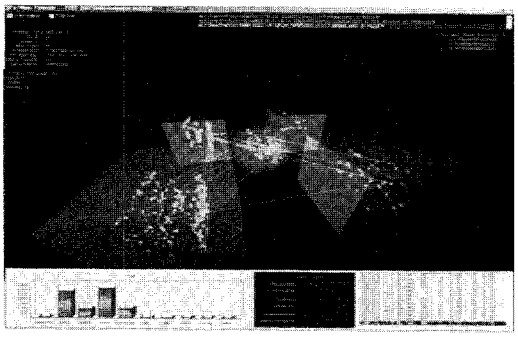
앞에서의 기술을 연동하고 각 관리자와 모듈들이 서로 협동과 조절을 통하여 모바일 단말의 보안을 관리한다. 이때 보안 상황과 모바일 단말의 위치와 자원이나 정보를 엑세스하는 과정을 3차원으로 시각화한다.

[그림 10]은 모바일 단말의 트래픽에 의한 보안 관리 상황을 모니터링하는 과정이다. 또한 [그림 11]은 주소

체계를 3차원 좌표 값으로 활용하여 모바일 단말기의 정보 접근 상황을 보이고 있다. 이 3차원 시각화는 관리자에 의해 뷰를 변경하면서 모니터링할 수 있다.



〔그림 10〕 모바일 단말 보안 관리 모니터링



〔그림 11〕 정보 접근 과정의 3차원 시각화 모니터링

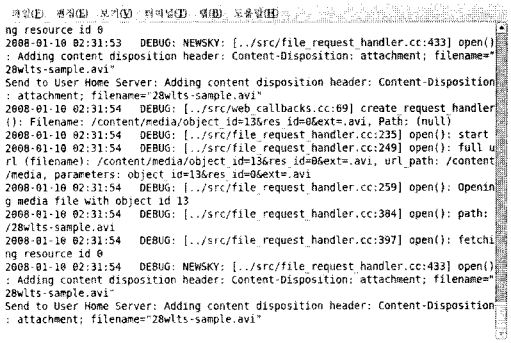
Ⅵ. 홈 엔터테인먼트에의 보안 응용 기술

이 절에서는 앞에서의 모바일 단말의 보안 관리 시스템을 모바일 단말이 이동하면서 홈 엔터테인먼트에 접속하고 콘텐츠를 모바일 단말로 끊임없이 재생하는 기술을 설명한다.

본 연구가 응용되는 홈 엔터테인먼트 시스템은 UPnP A/V 프레임워크 기반의 홈 서버이다. 이 서버에서 사용자는 컨트롤 포인터를 사용하여 미디어 서버에 있는 콘텐트를 미디어 랜더러로 재생한다. 기존 UPnP 환경에서의 서비스 제공자는 자신이 제공한 서비스를 누가, 언제 제공받았는지에 대하여 데이터베이스에 관리하고 있다. 그러므로 개인 프라이버시를 침해할 수 있는 문제점이 있다[7,10].

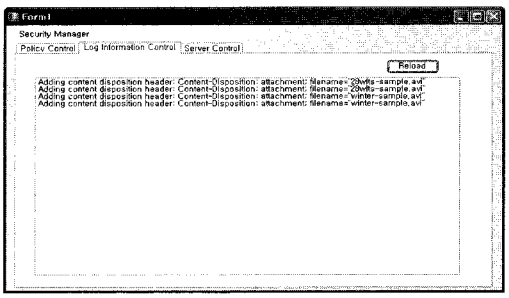
본 응용 기술에서는 컨트롤 포인터에서 미디어 서버로 콘텐트를 요청하면 미디어 서버는 컨트롤 포인터로부터 홈 도메인 서버에 대한 정보를 받는다. 해당 정보를 바탕으로 홈 도메인 서버의 사용자의 프라이버시 정책을 수신한다. 수신한 프라이버시 정책을 바탕으로 미디어 서버가 제공하는 접근 기록에서 홈 도메인 서버로 전송할 정보를 추출하고 전송한다.

[그림 12]는 미디어 서버가 접근 기록 정보를 저장하고 사용자의 홈 도메인 서버로 전송하는 부분이다.



〔그림 12〕 미디어 서버 동작

[그림 13]은 홈 도메인 서버에 서비스 제공자로부터 수신된 접근 기록 정보를 관리하는 화면이다.



〔그림 13〕 홈 도메인 서버의 접근 기록 관리

Ⅶ. 요 약

본 연구는 여러 위치에서 이동 중인 다양한 유형의 단말기에 대해 보안을 관리하는 통합 시스템을 국내 기술로 개발한 것이다. 특히 정부의 대학 IT 연구센터지원 사업의 결과라는 것은 의미 있는 일이다.

여기에 포함하는 기술 중에는 모바일 단말을 인증하는 과정, 단말을 신뢰하는 기술, 개인 접근 기록을 제어하는 기술, 3차원 모니터링 기술 등이 포함되어있다.

인증과 신뢰 기술은 다른 도메인에 접근하였던 단말이 이동하여 현 위치의 도메인에 접근하더라도 신뢰할 수 있는지를 검사한다. 이 기술은 서버와 서버, 단말과 서버 사이에서 신뢰도에 따라 이루어지는 중요 기술로 특허를 획득하였다. 다른 기술로 유비쿼터스 시대의 주요 문제인 프라이버시 침해를 방지하는 기술이 포함되어 있다. 이 프라이버시를 침해를 방지하는 기술 역시 특허를 출원한 상태이다. 또한 3차원 모니터링 기술 역시 특허를 출원한 상태이다.

이와 같이 특허를 출원하거나 등록할 수 있는 것은 이 연구가 중요하다는 의미이며 보안 관리 통합 시스템의 연구가 의미 있음을 알 수 있다. 이러한 기술을 응용하여 여러 기술을 파생하거나 파급할 수 있다.

참고문헌

[1] F.Almenarez, A.Marin, et al, "Developing a Model for Trust Management in Pervasive Devices," *Proceedings of the Fourth IEEE Conference on Pervasive Computing and Com-munications Workshop,* 2006.

[2] C.Lin, V. Varadharajan, et al, "Security and Trust Management in Mobile Agents: A New Perspective," *Proceedings of The Second International Conference on Mobile Technology, Application and Systems,* 15-17, November 2005.

[3] H. Jameel, L. Hung, et, al, "A Trust Model for Ubiquitous Systems based on Vectors of Trust Values," *Proceedings of the Seventh IEEE International Symposium on Multimedia,* 2005.

[4] D. McKnight and N. Chevany, "The Meanings of Trust," *Working paper, Carlson School of Management, University of Minnesota,* 1996.

[5] Y. Wang, F. Lin "Trust and Risk Evaluation of Transactions with Different Amounts in Peer-to-Peer E-Commerce Environments," *The IEEE International Conference on e-Business Engineering,* 2006.

[6] G. Anastasi, R. Bandelloni, M. Conti, F. Delmastro, E. Gregori, and G. Mainetto, "Experimenting an indoor bluetooth-based positioning service," *Proceedings of 23rd International Conference on Distributed Computing Systems Workshops*, pp. 480-483, 2003.

[7] 정의균, 김상욱, "유비쿼터스 환경에서 위치 인지 기반한 재생 장치 동적 전환 메커니즘", *한국정보처리 학회 추계학술발표대회 논문집*, 14(2), pp. 805-807, 2007.

[8] 서운석, 신순자, 구자동, 임진수 "유비쿼터스 컴퓨팅 환경에서 보안 및 인증서비스 방향 연구", *한국전산원*, 2004.

[9] 홍종현, "유비쿼터스 환경에서의 개인정보 보호", *Public Law Korean Public Law Association*, Vol. 32, No. 5, June 2004.

[10] 이제훈, 김상욱, "유비쿼터스 환경에서 프라이버시 보호를 위한 동적 접근 제어 시스템", *정보과학회 추계학술발표대회*, 34(2), pp. 118-121, 2007년 10월.

[11] S.Sackmann, J. Struker, R.Accorsi, "Personalization in Privacy-Aware Highly Dynamic Systems", *Communications of the ACM*, Vol. 49, No. 9, pp. 32-38, September 2006.

〈著者紹介〉

김 상 욱 (Sangwook Kim)
정회원

1979년 2월: 경북대학교 컴퓨터공학 학사
1981년 2월: 서울대학교 컴퓨터과학 석사
1989년 2월: 서울대학교 컴퓨터과학 박사
1988년 3월~현재: 경북대학교 전자전기컴퓨터학부 교수
<관심분야> 모바일 컴퓨팅