情報保護學會論文誌
第20卷 第1號, 2010. 2

시스템 명세화 기법 기반의 개인정보보호 모바일 알람 시스템 설계 및 구현*

장 은 영,† 김 형 종‡
서울여자대학교 컴퓨터학과

System Specification-based Design of Mobile Alarm System for Privacy Protection*

Eun Young Jang,† Hyung Jong Kim‡
Division of Computer, Seoul Women's University

요 약

시스템 명세 기법은 시스템의 구조와 행위특성을 형식적인 표현을 통해 제시하기위해 사용되는 시스템 이론 기반의 정형화된 표현 기법이다. 시스템 명세 기법을 시스템의 설계 단계에서 활용할 경우, 계층적이고 모듈화된 시스템에 대한 정의와 유지보수의 용이성 확보가 가능하여 합리적인 개발이 가능하게 된다. 본 연구에서는 개인정보 사용의 위험 상황을 모바일 장치를 이용하여 정보의 소유자에게 알려주고, 이에 대한 응답을 관리하는 기술을 제시하고 있다. 특히, 모바일 장치가 갖는 제약사항을 해결하기 위한 메시지의 형식을 정의하여 제시하였다. 본 기술이 적용된 알람 시스템은 계층적이고 모듈화된 형태로 모델링하기 위해 시스템명세를 기반으로 하였다. 또한, 시스템 명세화 기법 기반의 설계를 통해 알람시스템을 개발하고 본 시스템의 효율성을 검증 하였다. 본 논문의 기여도는 시스템명세기법을 사용한 개인정보 유출상황의 유연성 있는 표현과 관리를 가능하게 한 시스템의 설계 및 구현에 있다.

ABSTRACT

The system specification is a system theory based formal representation method for systems' structure and behavior modeling. When we make use of the system specification method in each step of software development, we can derive a hierarchical and modularized system design which enables us to manage the software development process flexibly. This research presents system specification based design of a mobile alarm system which sends alerts about illegal usage of private information and manages the response against the each alert. In our design of mobile alarm system, there are formal definition of alert message overcoming the functional limitation of mobile device and hierarchical modularized modeling of alarm processing using system specification. The efficiency of making use of the system specification is shown by applying the specification method to implementation of mobile alarm system. The contribution of this work is in design and implementation of mobile alarm system which enables us to handle the private information leakage situation more flexible way using system specification based software designing method.

Keywords: Mobile alarm system, System specification-based software design, Private information protection

I. 서 론

최근 컴퓨팅 환경에서의 다양한 서비스에서 활용되는 데이터 및 사용자의 개인정보에 대한 침해 위협이 증가하고 있다. 이러한 위협의 증가와 함께 개인정보를 중심으로 하는 서비스의 복잡도는 점점 증가되고 있으며, 이에 대한 침해사고 발생 시 효율적으로 대응

접수일(2009년 9월 24일), 수정일(2009년 11월 11일), 게재확정일(2009년 12월 10일)
* 본 연구는 2009학년도 서울여자대학교 교내학술특별연구비의 지원을 받았음.
† 주저자, elishajey@swu.ac.kr
‡ 교신저자, hkim@swu.ac.kr

하기 위한 개인정보보호 방법이 요구되고 있다.

본 논문에서는 이와 같은 기존 정보 관리 시스템의 단점을 보완하기 위해 시스템 명세화 기법을 기반으로 효율적으로 개인정보를 보호하는 개인정보보호정책 기반의 알람 시스템을 모델링 및 설계하였다. 시스템 명세기법은 시스템의 구조와 행위특성을 형식적인 표현을 통해 제시하기위해 사용되는 시스템 이론 기반의 정형화된 표현기법이다.

본 시스템은 모듈별 정형적 명세 기법을 통하여 설계 및 구현하였으며, 이 기법은 객체를 기능에 따라 모듈화하고 수학적으로 명세화하기 때문에 각각의 의미를 분명히 할 수 있다. 본 논문의 제안 방법에서는 사용자의 요구가 반영 가능한 개인정보보호를 위해 모바일 알람정보에 대해 정보소유자의 의견을 반영할 수 있게 하였다. 또한, 시스템을 계층적이며 객체 지향적인 정형화 명세를 통해 모델링하고 이를 기반으로 알람시스템을 설계 및 구현하여 유연하고 효율적인 개인정보관리를 방법을 제시하였다.

II. 관련연구

참고[2]의 시스템이론에서는 계층적 구조를 갖는 시스템 명세기법에 대한 시스템 명세의 계층을 시스템의 입출력 인터페이스를 묘사하는 하위 계층에서 형식적인 구조를 갖는 상위 계층을 7계층으로 구성하고 있다. 5계층의 구조적 시스템 명세에서 결합 시스템 명세는 $N = \langle T, X_N, Y_N, D, \{ M_d \mid d \in D \cup \{N\} \}, EIC, EOC, IC \rangle$와 같은 구조를 갖는다. 네트워크(N)에서의 입력(X_N), 출력(Y_N)과 동적 컴포넌트의 집합(D), 결합방식(EIC, EOC, IC)으로 표현한다. 또한, 외부 입력(EIC)과 출력(EOC), 내부(IC) 결합형식은 컴포넌트와 포트간의 결합으로 구성된다. 각 컴포넌트의 명세는 $M_d = (T, X_d, Y_d, \Omega, Q, \Delta, \Lambda)$와 같다. 시간단위로(T) 작동하는 컴포넌트는 입력과 출력이 있으며, 허용되는 각 세그먼트(Ω)는 각 함수(Δ)에 따라 상태(Q)가 결정되고 출력값을 결정하는 함수(Λ)는 입력 값과 세그먼트에 의해 결정된다.

참고[4]는 정책 기반의 개인정보보호와 관련된 법과 규칙, 그리고 개인정보관리 시스템을 제안한다. 정책기반 개인정보관리 시스템은 개인정보 보안 정책을 기반으로 개인정보를 자동으로 관리하며 보안성이 높고 신뢰할 수 있는 서비스를 제공한다. 이 시스템은 웹 환경에서 개인정보의 접근제어와 모니터를 통해 안전하게 개인정보를 관리하고 보호한다. 또한 정보요청과 정보사용이 있을 때, 자동으로 개인정보정책과 비교하는 기능으로 규칙적인 정보관리를 한다.

참고[5]의 시스템은 인터넷 환경에서 시스템 내부와 외부에서 발생하는 장애를 효율적으로 관리하기 위해 알람을 발생시킨다. 알람을 효과적으로 관리하기 위하여 장애 알람과 경보 알람으로 분류하고 이에 대한 요구사항을 연산하여 처리한다. 중요한 연결인 경우 장애를 복구하기위한 방법과 처리과정이 있으며, 알람 발생률에 따라 우선순위별 시간당 알람 상황을 처리하므로 우선순위가 낮은 알람은 우선순위가 높은 알람에 비해 처리 속도가 느릴 수 있다.

본 논문에서는 참고[2],[3]을 참고하여 개인정보보호 정책 시스템 및 정보관리 시스템과 독립적으로 상호작용하는 알람시스템의 모듈을 세부 기능별로 계층화하여 명세하였다. 또한, 참고[4]의 개인정보보호정책기반의 개인정보관리 시스템이 정책과 법, 규칙을 기반으로 결정하는 비정상적인 정보사용에 대한 알람과 정상적 정보사용이지만 사용자에 공개해야하는 알람을 표현하는 기술적 방법을 제안하였다. 본 시스템에서 발생하는 알람은 정책기반 시스템에서 발생하는 신호를 비정상, 비정상으로 의심되는 경고, 정상상황으로 분류하였고 각 상황에 따른 알람 처리 과정을 상세하게 명세화 한다는 점에서 참고[5]의 방법 보다 우수하다고 할 수 있다.

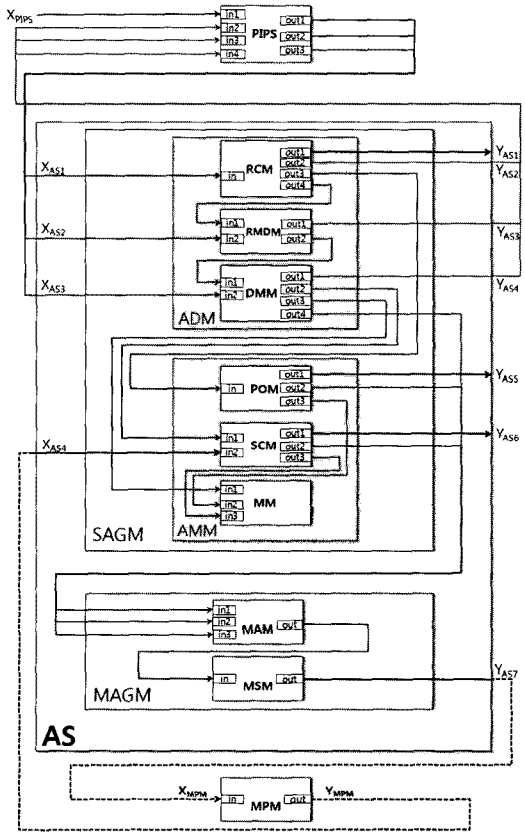
III. 시스템 명세 기법 기반의 알람 시스템 모델링

개인정보관리 시스템은 개인정보를 다량으로 보유하기 때문에 높은 보안성이 요구되는 시스템이므로 관리적 측면에서는 면밀한 보호와 관리가 필요시 되며, 사용자 측면에서는 정보 관리에 대한 공개와 개입을 요구한다. 그러나 기존의 개인정보관리는 정보소유자에게 정보관리를 공개하고, 승인받는 방법이 없어서, 개인정보의 관리적법성과 저장되는 개인정보의 정확성이 부족하다. 본 논문은 이러한 문제의 해결책으로 개인정보보호정책을 따르는 모바일 알람 시스템을 모듈단위로 명세화 하고 모델링하여 유연하게 알람을 제어할 수 있는 설계를 제시하고 있다.

3.1 알람 시스템의 구조적 결합 명세

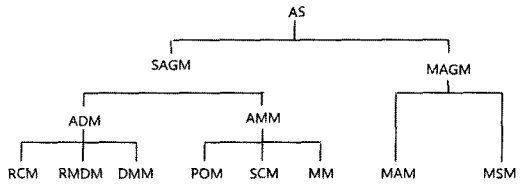
본 논문에서 제안하는 알람시스템의 입출력 설계는 [그림 1]과 같이 시스템 명세 기법을 기반으로 모델링

하였다[2][3]. 본 시스템은 개인정보관리 시스템과 개인정보보호 정책 시스템의 독립적인 연관관계를 고려한 모듈간의 독립적인 설계로 에러 수정과 기능 변경 및 추가가 용이하며, 계층적 모듈 명세를 통해 알람을 특성 별로 분류하여 알람 발생의 위험도에 따라 효율적인 관리가 가능하다. 또한 모바일의 사용자 인터페이스와 통신환경의 한계를 고려하여 단계별로 알람을 생성하고 알람의 특성을 상세히 명시함으로써 모바일장치를 통해 사용자의 대응의견을 수렴할 수 있게 하였다.



AS(Alarm System) : 알람 시스템
PIPS(Personal Information Policy System) : 개인정보보호정책 시스템
SAGM(System Alarm Generation Module) : 시스템 알람 생성 모듈
MAGM(Mobile Alarm Generation Module) : 모바일 알람 생성 모듈
ADM(Alarm Decision Module) : 알람 결정 모듈
AMM(Alarm Management Module) : 알람 관리 모듈
RCM(Risk Classification Module) : 위험 분류 모듈
RMDM(Response-Mode Decision Module) : 응답모드 결정 모듈
DMM(Detail Message Module) : 세부 메시지 모듈
POM(Priority Occupation Module):우선순위 선점 모듈
SCM(Signal Control Module) : 신호 제어 모듈
MM(Management Module) : 관리 모듈
MAM(Mobile Alarm Module) : 모바일 알람 모듈
MSM(Mobile Signal Module) : 모바일 신호 모듈
MPM(Mobile Privacy Management) : 모바일 개인정보 관리 프로그램

[그림 1] 알람 시스템 입출력 설계



[그림 2] 알람 시스템의 기능 구조

[그림 1]의 모듈들은 [그림 2]와 같이 계층구조로 표현될 수 있다. 가장 큰 분류로 알람이 생성되는 목적을 기준으로 SAGM, MAGM으로 나뉜다. SAGM은 시스템 내에서 알람을 구성하는 모듈이며, MAGM은 모바일 알람 형식으로 변경하는 모듈이다. SAGM은 알람을 결정하는 ADM과 알람을 관리하는 AMM으로 구분된다. ADM은 위험도를 결정하는 RCM, 사용자의 모바일 대응 가능 여부를 결정하는 RMDM, 상세메시지를 결정하는 DMM으로 구성된다. AMM은 알람 관련정보 관리의 우선순위를 결정하는 POM, 모바일 대응 신호를 관리하는 SCM, 모든 알람 관련정보를 관리하기 위한 MM으로 구성된다. MAGM은 모바일알람을 형성하고 관리하는 MAM과 모바일 알람을 무선 통신 신호로 변환하여 모바일 알람메시지를 전송하는 MSM으로 구성된다. 각 모듈의 기능을 계층적으로 모델링함으로써 정보관리 시스템에 유연한 적용이 가능하며, 알람 상황을 체계적이며 효율적으로 관리 할 수 있다.

아래 [표 1]의 시스템명세와 같이 AS는 시간단위(T)로 알람을 발생하는 시스템으로 네트워크의 외부 입력(X_{AS})과 출력(Y_{AS})으로 구성된다. PIPS에서 적용한 개인정보보호정책을 기반으로 사용자의 접근이나 개인정보 활용에 대해 결정된 결과 값은 [표 1]의 결합명세와 같이 외부 네트워크 연결(EIC)을 통해 AS로 입력된다. PIPS와 연동되는 외부 입력 값은 PIPS의 개인정보정책을 위배하여 정보 활용이 거부된 경우이거나 합법적이므로 정보 활용이 승인된 경우이나 승인이 필요한 값(X_{AS1}), AS에서 알람을 형성하기위해 요청하여 PIPS가 전달한 값(X_{AS2}, X_{AS3})이다. 그리고 그 외 모바일 알람메시지에 대해 사용자가 참여한 개인정보 사용 동의 및 거부 의견(X_{AS4})으로 구성되어있다. AS는 알람 상황을 파악하기 위해 외부

네트워크 연결(EOC)을 통해 필요한 알람 관련 정보 값을 PIPS에게 요청하고 전달하며, 이를 기반으로 사용자의 접근이나 개인정보 활용에 대한 결과 값을 출력한다. AS의 외부 출력 값은 사용자의 동의와 확인이 필요하지 않은 합법적인 개인정보 활용에 대한 결과 값(Y_{AS1})과 PIPS에서 발생한 개인정보 활용에 대한 판정을 개인정보정책에 기준하여 각 모듈의 역할에 맞게 알람을 분류하기 위해 PIPS에게 알람의 속성을 요청하는 값(Y_{AS2}, Y_{AS3}, Y_{AS4}), 개인정보 사용을 승인하지 않는 값(Y_{AS5}), 사용자의 의견을 반영하여 정보 활용여부가 결정된 값(Y_{AS6}), 모바일에 알람을 보내는 값(Y_{AS7})이다. 이러한 방식은 PIPS와 AS간의 상호결합이 가능한 프로토콜이 요구되며 다양한 시스템에 적용하기 위해 필요한 요구방식이다. 또한 알람 상황을 선별하고, 모바일 장치에 알람메시지를 보내고 모바일 장치를 통해 전달되는 사용자의 의견을 수렴하는 것을 가능하게 한다.

AS의 모듈 집합(D)은 SAGM과 MAGM으로 구성된다. PIPS에서 입력되는 값은 AS의 내부 모듈간의 연결(IC)을 통해 분류되고 관리된다. AS의 외부 입력포트의 범위는 [표 1]의 모듈 간 결합관계와 같이 SAGM의 외부 입력포트 범위에 포함되며, SAGM과 MAGM의 외부 출력포트의 범위는 AS의 외부 출력포트 범위에 포함된다. 또한 SAGM의 내부출력포트 범위가 MAGM의 내부입력 포트의 범위에 포함된다.

[표 1] 알람시스템의 구조 및 결합 명세

시스템 명세	$AS = \langle T, X_{AS}, Y_{AS}, D, \{M_{SAGM}, M_{MAGM} \mid SAGM, MAGM \in D\}, EIC, EOC, IC\rangle$ $X_{AS} = (IPorts_{AS}, X_{AS1} \times X_{AS2} \times X_{AS3} \times X_{AS4})$ $Y_{AS} = (OPorts_{AS}, Y_{AS1} \times Y_{AS2} \times Y_{AS3} \times Y_{AS4} \times Y_{AS5} \times Y_{AS6} \times Y_{AS7})$
결합 명세	$EIC \subseteq \{((AS, ip_{AS}), (SAGM, ip_{SAGM})) \mid ip_{AS} \in IPorts_{AS}, SAGM \in D, ip_{SAGM} \in Iports_{SSAGM}\}$ $EOC \subseteq \{((SAGM, op_{SAGM}), (AS, op_{AS})) \mid SAGM \in D, op_{SAGM} \in Oports_{SSAGM}, op_{AS} \in OPorts_{AS}\}$ $EOC \subseteq \{((MAGM, op_{MAGM}), (AS, op_{AS})) \mid MAGM \in D, op_{MAGM} \in Oports_{MAGM}, op_{AS} \in OPorts_{AS}\}$ $IC \subseteq \{((SAGM, op_{SAGM}), (MAGM, op_{MAGM})), \mid SAGM, MAGM \in D, op_{SAGM} \in Oports_{SSAGM}, ip_{MAGM} \in Iports_{MAGM}\}$
결합관계 명세	$\forall((AS, ip_{AS}), (SAGM, ip_{SAGM})) \in EIC : range_{eip_{AS}}(X_{AS}) \subseteq range_{ip_{SAGM}}(X_{SAGM})$ $\forall((SAGM, op_{SAGM}), (AS, op_{AS})) \in EOC : range_{eop_{SAGM}}(Y_{SAGM}) \subseteq range_{op_{AS}}(Y_{AS})$ $\forall((MAGM, op_{MAGM}), (AS, op_{AS})) \in EOC : range_{eop_{MAGM}}(Y_{MAGM}) \subseteq range_{op_{AS}}(Y_{AS})$ $\forall((SAGM, op_{SAGM}), (MAGM, ip_{MAGM})) \in IC : range_{op_{SAGM}}(Y_{SAGM}) \subseteq range_{ip_{MAGM}}(X_{MAGM})$

[표 2] 알람시스템 모듈의 주요 구조적 명세

시스템 명세	$M_{SAGM} = \langle T, X_{SAGM}, Y_{SAGM}, D_{SAGM}, \{ M_{ADM}, M_{AMM} \mid ADM, AMM \in D_{SAGM} \}, EIC, EOC, IC\rangle$ $M_{ADM} = \langle T, X_{ADM}, Y_{ADM}, D_{ADM}, \{ M_{RCM}, M_{RMDM}, M_{DMM} \mid RCM, RMDM, DMM \in D_{ADM} \}, EIC, EOC, IC\rangle$ $M_{AMM} = \langle T, X_{AMM}, Y_{AMM}, D_{AMM}, \{ M_{POM}, M_{SCM}, M_{MM} \mid POM, SCM, MM \in D_{AMM} \}, EIC, EOC, IC\rangle$ $M_{MAGM} = \langle T, X_{MAGM}, Y_{MAGM}, D_{MAGM}, \{ M_{MAM}, M_{MSM} \mid M_{MAM}, M_{MSM} \in D_{MAGM} \}, EIC, EOC, IC\rangle$ $M_{RCM} = \langle T, X_{RCM}, Y_{RCM}, \Omega, Q, \Delta, \wedge\rangle$ $M_{RMDM} = \langle T, X_{RMDM}, Y_{RMDM}, \Omega, Q, \Delta, \wedge\rangle$ $M_{DMM} = \langle T, X_{DMM}, Y_{DMM}, \Omega, Q, \Delta, \wedge\rangle$ $M_{POM} = \langle T, X_{POM}, Y_{POM}, \Omega, Q, \Delta, \wedge\rangle$ $M_{SCM} = \langle T, X_{SCM}, Y_{SCM}, \Omega, Q, \Delta, \wedge\rangle$ $M_{MM} = \langle T, X_{MM}, Y_{MM}, \Omega, Q, \Delta, \wedge\rangle$ $M_{MAM} = \langle T, X_{MAM}, Y_{MAM}, \Omega, Q, \Delta, \wedge\rangle$ $M_{MSM} = \langle T, X_{MSM}, Y_{MSM}, \Omega, Q, \Delta, \wedge\rangle$

[표 2]의 시스템명세와 같이 SAGM, MAGM에서 시간 단위로 발생하는 각 외부 입력(X_{SAGM}, X_{MAGM})은 세부 모듈(M_{RCM}, M_{RMDM}, M_{DMM}, M_{POM}, M_{SCM}, M_{MM}, M_{MAM}, M_{MSM})의 외부네트워크 연결과 내부네트워크 연결로 이루어진 프로세스를 통해 외부 출력(Y_{SAGM}, Y_{MAGM})이 결정된다. SAGM은 시스템에서 알람을 생성하는 모듈로 알람을 결정하는 ADM과 관리하는 AMM으로 구성된다. ADM의 외부네트워크 연결을 통한 입력 값(X_{ADM})은 [표 1]의 X_{AS1}, X_{AS2}, X_{AS3}과 같으며, 출력 값(Y_{ADM})은 [표 1]의 Y_{AS1}, Y_{AS2}, Y_{AS3}, Y_{AS4}과 같은 외부 출력 값과 AMM과 내부 결합(IC)되는 값으로 구성된다. AMM은 외부 입력 값이 [표 1]의 X_{AS4}과 같으며, ADM에서 내부 결합(IC)으로 전달되는 값이 내부 입력된다. 외부 출력 값은 [표 1]의 Y_{AS5}, Y_{AS6}과 같으며 MSGM과 내부 결합(IC)을 통한 내부 출력 값이 있다. 모바일 알람을 생성하는 MAGM은 모바일 메시지를 전달하는 무선통신을 하기 위한 MAM과 MSM로 구성된다. MAGM의 입력 값(X_{MAGM})은 MAM을 통해 ADM과 AMM에서 내부 결합(IC)으로 전달되는 값으로 모바일 알람메시지를 전송하기 위해 완성된 알람 값이며, 결과 값(Y_{MAGM})은 MSM을 통해 출력되는 모바일 알람메시지로 [표 1]의 Y_{AS7}과 같다.

최하위 모듈들(M_{RCM}, M_{RMDM}, M_{DMM}, M_{POM}, M_{SCM}, M_{MM}, M_{MAM}, M_{MSM})은 [표 2]와 같이 기본

적인 입출력, 시간 속성 외에 모듈별 입력 세그먼트(Ω), 상태집합(Q), 상태전이함수(Δ) 및 출력함수(∧)를 갖는다.

RCM, RMDM, DMM은 PIPS에서 발생하는 신호를 기반으로 출력을 결정한다. RCM은 [표 3]과 같이 개인정보에 대한 접근을 정상, 비정상에 따라 침해, 경고, 확인 상황으로 분류하는 모듈이다. 이러한 상황분류는 위험에 따라 우선순위로 위험상황을 관리하거나 알람메시지를 전송하기 위한 것이다. 본 모듈의 외부출력은 정보 활용이 정상이며 사용자의 확인과 의견 수렴이 필요 하지 않은 값이다. RMDM은 사용자가 위험상황을 모바일 단말을 통해 제어 가능한지 여부로 분류한다. 양방향 알람은 사용자가 모바일 장치를 이용하여 개인정보 정보 활용을 제어할 수 있으며, 단방향알람은 개인정보 침해 시 오직 관리자만이 제어 가능한 상황이거나 제약적 환경을 가진 모바일 장치를 이용하여 알람 상황에 대한 확인 및 제어가 불가능한 상황이다. DMM은 작은 메모리와 제한된 사용자 인터페이스로 인해 콘텐츠 제공이 한정된 모바일 환경을 위해 알람 상황에 대한 세부 정보를 제공하는 모듈이다. 이 기능으로 인해 사용자는 모바일단말을 이용하여 개인정보보호의 알람 상황에 대해 'true/false'의 응답으로 만으로 쉽게 대응 할 수 있다.

[표 3] 알람의 위험 및 관리 우선순위 분류

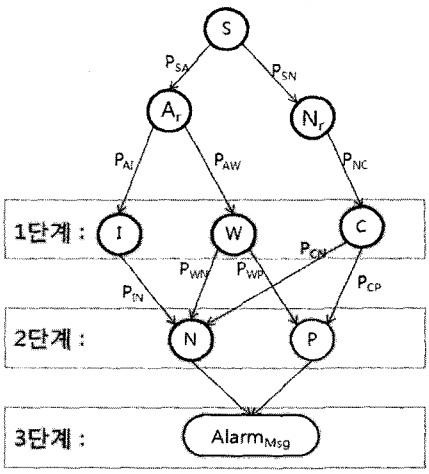
위험 분류	설명	우선 순위
침해(I)	비정상 접근	1
경고(W)	비정상 의심 접근	2
확인(C)	정상 접근 사용자 확인필	3

POM은 [표 3]의 위험도 분류에서 개인정보 유출 및 침해 상황에 대한 정보관리의 우선순위를 최상으로 선점한다. POM의 외부 출력 값은 개인정보 침해가 발생된 상황을 알리는 값으로 사용자의 확인이 필요하며, 사용자 응답 기반으로 관리자의 관리가 필요한 상황이다. SCM은 모바일 대응 시그널을 제어하는 모듈로 양방향 모바일 메시지와 관련된 정보 활용의 수행을 대기시키고, MAM을 통해 모바일 알람메시지를 전달한다. 일정시간 동안 대기 후, 외부에서 입력되는 사용자의 모바일 대응 의견을 기반으로 정보 활용 여부 결정한다. MM은 모든 알람 상황에 대한 정보를 우선순위에 따라 관리하는 모듈이다.

MAGM의 MAM은 모바일 메시지를 보내기 위해 MSGM에서 분류한 알람을 출력해주는 모듈이다. MAM은 알람을 모바일로 전달 가능한 메시지로 형성하며, 모바일 메시지 문자열은 MSM을 통해 모바일로 송신 가능한 무선데이터 신호로 변환한다.

본 논문은 참고[1]을 확장하여 시스템 명세화 기법을 기반으로 각 모듈을 기능단위로 모델링하고 개인정보보호 정책 시스템에서 발생하는 모든 신호를 알람시스템에서 발생 시킬 수 있도록 입출력을 재 정의하여 각 모듈간의 실행과정을 객체 단위로 구성하였다. 그러므로 본 논문은 이러한 설계를 통해 모듈의 구성이나 각각의 모듈 변경에 대해 독립적이고 유연한 특성을 갖는 시스템의 구성을 제시하고 있다. 이와 같은 구성으로 알람시스템에서 개인정보보호정책에 따라 알람을 생성하고, 개인정보소유자가 모바일 알람메시지와 모바일 단말기를 통해 정보관리에 대한 확인 및 응답으로 직접적인 개입이 가능하여 개인정보에 대한 안전성이 높아진다. 이러한 구성은, 사용자는 본인 정보 활용에 대한 알 권리를 충족하며, 관리자는 사용자가 승인한 개인정보 사용에 대해 부인봉쇄가 가능해진다.

3.2 모바일 알람 메시지 구조



S(Signal):개인정보보호정책시스템에서 발생하는 신호
Ar (Abnormal-request) : 비정상적인 개인정보 요청
Nr (Normal-request) : 정상적인 개인정보 요청
I(Invaded) : 개인정보 유출
W(Warn) : 개인정보 유출될 수 있는 경고
C(Confirm) : 개인정보 활용 동의 및 확인 필요
N(Non-participation) : 정보관리에 대해 참여 불가능
P(Participation) : 정보관리에 대해 참여 가능

[그림 3] 모바일 알람의 단계별 내용

모바일 알람메시지는 실시간으로 이동환경에서 확인하기 위해 보편화된 모바일 단말로 제공되는 알람서비스이다. 본 연구의 모바일 알람메시지는 OECD 개인정보보호 8대원칙에 위배될 수 있는 모든 상황을 내포하고 있으며 그 상황을 해결할 수 있는 모바일 개인정보관리 프로그램과 연계된다[1]. [그림 1]의 알람시스템 모듈간의 알람메시지 생성과정은 [그림 3]과 같이 계층적 트리구조를 갖는다. 트리의 1, 2 및 3단계는 알람결정모듈(ADM)에 의해 진행되는 과정에 해당되며, OECD 개인정보보호 8대원칙을 기반으로 하여 알람메시지를 "생성"한다.

$$Alarm_{Msg} = \{(risk, user) | risk \in \{I, W, C\}, user \in \{P, N\}\} \quad (1)$$

$$, where \\ \text{if } risk \equiv I \text{ then } user := N$$

본 논문에서 제안하는 알람메시지 결정트리는 알람의 개인정보를 요구한 상황을 정상, 비정상상황에 따라 Nr(정상), Ar(비정상)으로 분류된다(P_{SA}, P_{SN}).

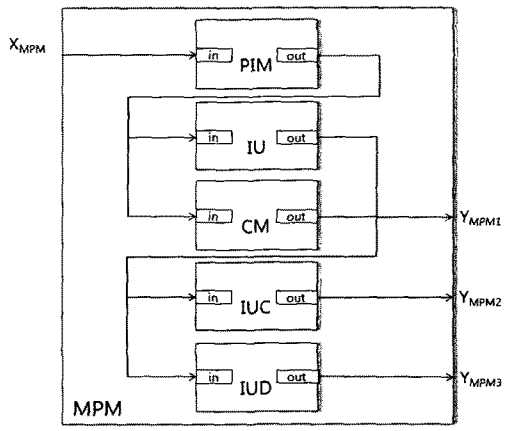
수식(1)과 같이 1단계의 RCM은 알람의 위험도에 따라 I(침해), W(경고), C(확인)의 알람메시지를 구분하고(P_{AI}, P_{AW}, P_{NC}) 2단계의 RMDM에 의해 개인 참여가능 여부에 따라 메시지를 P(참여 가능), N(참여 불가능)으로 구분한다(P_{IN}, P_{WN}, P_{WP}, P_{CN}, P_{CP}). 침해, 경고, 확인의 메시지 타입은 중복 존재 하지 않으며, 개인정보 침해는 정보관리에 대해 참여 불가능에 포함되고, 경고, 확인 메시지는 정보관리에 대해 참여 가능과 불가능에 모두 포함된다. 3단계는 DMM이 데이터 표현이 제한된 모바일 환경을 고려하여 상세하게 알람상황을 구성한 $Alarm_{Msg}$를 생성한다. 이로써 사용자가 위험 상황을 모바일로 인식하여, 실시간으로 간편하게 모바일 개인정보관리 프로그램을 통해 "true/false"방식으로 대응이 가능하다.

생성된 메시지는 MAGM에서 모바일 단말에 적합한 메시지형식과 모바일 신호로 "변경"하여 정보소유자의 모바일 단말기로 모바일 알람메시지를 "송신"된다.

메시지 생성이 완료되면, AMM에 의해 알람 메시지의 송신과 알람 상황을 위험도의 우선순위에 따라 단계적으로 해당 위험에 대해 "관리"를 수행하고, 동시에 모바일 사용자의 참여를 개인정보 관리에 반영한다.

3.3 모바일 개인정보관리 프로그램의 구조적 명세

본 논문에서 제안하는 알람시스템은 높은 수준의 개인정보보호가 요구되는 시스템에 도입되어야 하는 모델이다. 가치 있는 정보의 보안을 높이기 위해서 정보소유자가 개인정보관리에 개입한다. 즉, 사용자는 AS에서 송신되는 모바일 메시지(Y_{AS7})에 대해 MPM을 통해 사용자의 동의 및 거부 의견(X_{AS4})을 AS로 전달한다.



MPM(Mobile Privacy Management) : 모바일 개인정보관리 프로그램
PIM(Personal Information Management):개인정보관리
IU(Information Usage) : 정보사용 관리
CM(Certification Management) : 인증서 관리
IUC(Information Usage Confirm) : 정보사용 동의
IUD(Information Usage Deny) : 정보사용 거부

[그림 4] 모바일 개인정보관리 프로그램 입출력 설계

[그림 4]와 같이 MPM의 PIM의 출력은 CM과 IU의 입력으로 내부네트워크연결(IC)되어 있다. CM는 모바일인증서를 발급, 갱신, 폐기, 변경, 확인하는 역할을 하는데, 이러한 모바일인증방식은 참고[1]의 모바일 개인정보관리 프로그램에서 알람시스템에 전달하는 개인정보가 누출될 수 있음을 고려하여 적용되었다. IU는 IUC와 IUD와 내부네트워크(IC)로 연결되어 있는데, 이는 관리자 측면에서 모바일 프로그램에서 전달되는 대응신호의 우선순위를 결정하기위해 분리한 것으로 같은 시간에 IUD에서 전달하는 신호의 우선순위가 IUC보다 높게 설정된다. 또한 신호는 'true/false'로 구성되어 비전문가인 사용자가 의사결정을 쉽게 할 수 있게 하였다.

IV. 시스템 구현

4.1 알람시스템 구현

Alarm System

RCM(Signal ①Y_{PIPS})
②Signal X = Y_{PIPS}==normal? normal : abnormal
if(X == normal)
③X += Y_{PIPS}==Confirm ? Confirm : normal else
③X += Y_{PIPS} ==Warn ? Warn : Invaded
if(X != normal + Confirm)
⑦Positive_output//개인정보 활용 승인
else if(X == normal + Confirm)
④RMDM(X)
else if(X = = abnormal + Warn)
RMDM(X)
else
POM(X)

RMDM(Signal X)
X += X == oneway? oneway : twoway
DMM(X)

DMM(Signal X)
X +=PIPS(X==X.messageType ? X.message);
MSG = Select DB(X)
if(X = = one way)
{
⑤MAM(MSG)//단방향일 때 모바일 메시지
MM(X)
}
else if(PIPS(X) = = two way)
⑤SCM(MSG)

POM(Signal X)
MSG = Select DB(X);
⑤MAM(MSG)//정보 유출일 때 모바일 메시지
MM(X)
X.number = 1
⑦Negative_output//개인정보 활용 불승인

SCM(Signal MSG, Signal Y)
⑤MAM(MSG)//양방향일 때 모바일 메시지
MM(X)
⑥while(inTimeSec(180))
{
if(Y = = C)
⑦Positive_output//개인정보 활용 승인
else
⑦Negative_output//개인정보 활용 불승인
}
⑦Negative_output//개인정보 활용 불승인

MM(Signal X)
for(int i = 1; i <= X.number ; X.number++)
manage X//우선순위 관리

MAM(Signal MSG)
MSM(MobileMSG(MSG))//모바일 메시지로 변환

MSM(Signal X)
change MobileSignal(X)
⑦Alarmmessage_ouput//모바일 메시지 전송

〔그림 5〕 알람시스템 알고리즘

본 논문에서는 각 객체 모듈을 명세화하고 모듈 간 결합을 통한 구조적 시스템 명세화를 통해 각각의 특성에 따라 모듈을 구성하여 프로세스를 세분화하였다. 각 모듈들은 개인정보보호정책 시스템과 독립적으로 구성되었으며, 실시간으로 개인 정보 활용에 대한 정보를 교환한다.

〔그림 1〕의 알람시스템 모델링을 〔그림 5〕와 같이 구현하였다. 〔그림 5〕의 ①은 RCM에 개인정보 유출과 관련한 최초 출력 값이 입력되는 상황을 나타낸다. 〔그림 5〕의 ②를 보면 이 값을 기준으로 알람을 분류하게 되는데 RCM과 RMDM, DMM은 PIPS와의 지속적으로 통신하여 〔그림 5〕의 ③과 같이 알람에 대한 속성 값을 얻게 된다. 이러한 과정을 통해 얻는 값을 〔그림 5〕의 ④와 같이 순차적으로 전달하여 알람에 대한 상세정보를 조합한다. 사용자의 동의나 거부가 필요한 알람상황이라면 〔그림 5〕의 ⑤와 같이 모바일 알람메시지를 보내고, 사용자는 〔그림 5〕의 ⑥과 같이 특정 제한 시간 동안의 모바일을 통한 개인 참여로 인해 개인정보 활용을 결정한다. 위와 같은 실행과정을 거쳐 〔그림 5〕의 ⑦과 같이 개인정보 활용을 승인하거나 불승인하는 것으로 하나의 알람 프로세스가 종료된다.

4.2 모바일 개인정보관리 프로그램 구현

모바일 개인정보관리 프로그램의 소스코드 구성은 〔그림 6〕과 같다. 사용자는 개인정보관리 프로그램인 PIM의 IU에서 개인정보 사용 인증을 통해 개인 정보 활용에 대한 사용자의 참여가 가능하다. 참고〔1〕의 모바일 개인정보관리 프로그램은 개인정보보호 시스템의 아이디와 비밀번호 모바일 인증번호를 요구했으며, 출력이 "승인여부/아이디/비밀번호"로 전달되었다. 본 논문에서는 불필요한 개인정보보호 시스템의 비밀번호의 입력과 출력이 누출될 수 있음을 고려하여 〔그림 6〕의 ①과 같이 모바일 아이디와 비밀번호 입력을 통해 사용자를 인증하고 〔그림 6〕의 ②와 같이 동의나 거부 시에 'true/false'로 출력되는 프로그램으로 개선하였다. 또한 사용자의 동의를 전달하는 IUC와 거부를 전달하는 IUD를 분류하여, 시스템에 같은 시간에 전달되는 사용자의 의견을 처리하는 우선순위를 다르게 하였다. 이는 모든 알람 상황에서 사용자가 알람 메시지의 내용에 대해 거부하는 상황이 더 위험한 상황임을 고려한 것이다.

```
Mobile Privacy Management Program
PIM( )
if(select(help))
   view helpView
else if(select(IU))
   IU
else
   CM
IU( )
if(select(ConfirmView))
   IUC
else if(select(PreventionView))
   IUD
IUC(ID, mobilePWD)
①if(mobilePWD == getMobilePWD && ID == getID)
{
   ②send opinion(True)
   if( Receive from AlarmSystem opinion == OK)
      view successView
}
else
   view failView
IUD(ID, mobilePWD)
①if(mobilePWD == getMobilePWD && ID == getID)
{
   ②send opinion(False)
   if(Receive from AlarmSystem opinion == OK)
      view successView
}
else
   view failView
```

〔그림 6〕 모바일 개인정보관리 프로그램 알고리즘

V. 결론

본 논문에서는 참고[1]의 모바일 알람 시스템을 시스템 명세화 기법을 기반으로 확장하고 모델링함으로써 모듈의 특성과 입출력을 재 정의하여 개인정보보호 시스템과 독립적인 적용을 가능하게 하였다. 게다가 알람시스템의 기능 변경 및 추가가 용이하므로 정보보안시스템에서 필요시 되는 안전성이 확보된다. 그러므로 계층적이고 모듈화된 기술적 방법으로 설계되고 구현된 본 알람시스템은 모바일 알람메시지를 체계적으로 제공함으로써, 개인정보 관리가 정보보호정책을 준수하는 것을 증명할 수 있으며 사용자에게는 개인정보보호에 대한 알권리를 보장한다. 또한, 사용자가 모바일 개인정보관리 프로그램을 통해 개인정보를 관리에 의무를 다함으로써 관리자가 관리해야하는 정보량이 감소하고 시스템의 비정상적인 접근을 제어할 수 있어 개인정보 관리의 효율성과 보안성을 향상시킨다. 또한 모바일 개인정보관리 프로그램은 모바일 인증서로 본인을 인증하는 방식으로 재구성하여 보안성을 높였다. 향후에는 실제 개인정보보호정책 시스템의 입력과 출력을 분석하고 분류하여 본 논문에서 제안한 알람 시스템 설계가 실제 환경에서 어떠한 긍정적인 효과를 주는지 시뮬레이션을 통해 통계적으로 증명할 것이다.

참 고 문 헌

[1] 장은영, 김형종, 황준, "개인정보 관리를 위한 메시지 트리 기반의 모바일 알람 시스템 구축," 정보보호학회논문지, 19(3), pp. 153-162, 2009년 6월.

[2] B.P. Zeigler, H. Praehofer, and T.G. Kim, Theory of Modeling and Simulation, 2th Ed., Academic Press, Jan. 2000.

[3] 김은하, 조대호, "시스템 형식론에 의한 사용자 인터페이스 시스템 표현과 DEVS 모델링," 한국시뮬레이션학회논문지, 8(4), pp. 137-154, 1999년 12월.

[4] S.P. Hong, S.M. Kang, K.G. Kim, and J.H. Jeoung, "Prototyping the Privacy-Based Policy Management System for Securely Using Privacy Information," WISA 2009, pp. 121-129, Aug. 2009.

[5] J. Niinimäki, A. Holopainen, J. Kerttula, and J. Reponen, "Security Development of a Pocket-Sized Teleradiology Consultation System," Studies in Health Technology and Informatics, pp. 1266-1270, Aug. 2001.

[6] N.M. Karnik and A.R. Tripathi, "Security in the Ajanta Mobile agent system," Software-Practice & Experience archive, pp. 301-329, May 1999.

[7] I. Mavridis and G. Pangalos, "Security Issues in a Mobile Computing Paradigm," Informatics 97 security issues, pp. 61-76, Sep. 1997.

[8] J. Burkhadrdt, T. Schaeck, S. Happer, K. Rindtorff, and T. Schaeck, "Pervasive computing: Technology and Architecture of mobile internet applications," Addison-Wesley Longman Publishing Co, Jan. 2001.

[9] B. Lee, "Users' Perspective on Regulation to Protect Privacy on the Web," The International Information & Library Review, pp. 379-402, Sep. 2000.
[10] R. Sekar and P. Uppuluri, "Synthesizing Fast Intrusion Prevention / Detection Systems from High-Level Specifications," Proceedings of the 3rd USENIX Windows NT Symposium, pp. 12-15, July 1999.
[11] 한영태, 민덕기, "이벤트 알림 서비스의 구조설계와 성능분석," 한국시뮬레이션학회 추계학술대회논문집, pp. 95-103, 2003년 11월.

〈著者紹介〉

장 은 영 (Eun young Jang) 학생회원
2008년: 서울여자대학교 정보통신공학부 멀티미디어통신공학과(공학사)
2009년~현재: 서울여자대학교 일반대학원 컴퓨터학과 석박사통합과정
〈관심분야〉 시스템 이론기반 접근제어, 취약점 분석 및 모델링

김 형 종 (Hyung Jong Kim) 종신회원
1996년: 성균관대학교 정보공학과(공학사)
1998년: 성균관대학교 정보공학과(공학석사)
2001년: 성균관대학교 전기전자 및 컴퓨터공학과(공학박사)
2001년~2007년: 한국정보보호진흥원(KISA) 수석연구원
2004년~2006년: 미국 카네기멜론대학(CMU) 방문연구원
2007년~현재: 서울여자대학교 컴퓨터학부 조교수
2009년~현재: 한국시뮬레이션학회 논문지 편집위원장
〈관심분야〉 취약점 분석 및 모델링, 이산사건 시뮬레이션 방법론, 인터넷전화 보안기술