2007年度
韓國情報保護學會
冬季學術大會

CISC W'07 PROCEEDINGS

■ 일 시 : 12월 1일(토) 09:00 ~ 18:00
■ 장 소 : 상명대학교(서울 본교)

CISC 2007

Conference on
Information Security
and Cryptology

社団法人 韓国情報保護學会
KOREA INSTITUTE OF INFORMATION SECURITY & CRYPTOLOGY

- 주 관 : 한국정보보호학회
- 주 최 : 상명대학교
- 후 원 : 상명대학교, 한국과학기술단체총연합회, 고려대BK21 유비쿼터스 정보보호연구단,
- 협 찬 : 한국정보보호산업협회, 고려대 정보보호기술연구센터(CIST),
  성균관대 ITRC, 충남대 인터넷침해대응연구센터,
  중앙대 홈네트워크연구센터, 경북대 이동네트워크 정보보호기술연구센터,
  (주)마크애니, 시큐아이닷컴(주), (주)파수닷컴, (주)이글루시큐리티,
  (주)위너다임, (주)니트젠

목차

유비쿼터스 환경에서 프라이버시 컨트롤 프레임워크

이제훈* 김상욱

*경북대학교 전자전기컴퓨터학부

A Pricacy Control Framework in the Ubiquitous Environment

J.Lee* and S.Kim

*School of Electrical Engineering and Computer Science

Kyungpook National University.

요 약

도메인간의 이동이 빈번한 유비쿼터스 환경에서 다양한 디바이스를 통해서 서비스를 제공받을 때 서비스 제공자는 접근이나 동작 등의 기록을 남기게 된다. 그 기록으로 인하여 개인의 위치나 행동 등의 프라이버시가 보호받지 못하게 된다. 이러한 문제를 해결하기 위해서 접근 기록을 개인이 관리할 수 있는 적극적인 형태의 프라이버시 관리 시스템을 제안한다. 접근 기록을 사용자가 직접 관리하는 관리자로 전송하고 그 관리자를 통하여 분하는 수준의 정보만을 제공할 수 있도록 한다.

I. 서론

도메인간의 이동이 빈번한 유비쿼터스 환경에서 자유로운 이동을 위하여 개인의 정보는 개인이 알지 못하는 사이에 다른 도메인으로 넘어가게 된다[1]. 이러한 유비쿼터스에서의 프라이버시에 대한 접근은 동기으로 제안된 인증기나 개인 정보를 활용하여 상황에 맞는 컨텐츠를 제공하는 방향으로의 연구가 많이 되었다.

일반적인 환경에서 서비스 제공자들은 자신의 서비스를 제공함에 있어서 과금이나 행동 패턴 추적 등을 위해서 사용자의 정보를 서비스 제공자가 기억하고 있다. 사용자는 개인 정보를 제공한 다음에 그 정보를 바탕으로 어떠한 컨텐츠를 제공하였는지, 어떠한 행동을 하였는지에 대한 기록이 남아지는 지에 대해서는 전근하지는 고려하지 않았다. 또한 개인 정보를 보호함에 있어서 적절한 보안이 적용되어 관리되는지는 고려하지 않았다. 하지만 유비쿼터스 환경에서는 수많은 센서들이 존재하고 그곳에서 만들어지는 로그를 통하여 개인의 위치를 추적하고 행동을 예측할 수 있는 수준으로 기술이 발전하고 있다.

따라서 본 논문에서는 유비쿼터스 환경에서의 프라이버시를 설정하고 그러한 프라이버시를 보호할 수 있는 프레임워크를 제안한다. 프라이버시를 보호하기 위하여 다양한 서비스 제공자들이 관리하는 접근기록을 수집하여 사용자가 브라우징 한다.

본 논문의 구성에서는 기존의 연구에 대해서 살펴본다. 3장에서는 유비쿼터스 환경에서의 프라이버시를 설정하고 4장에서 프라이버시 보호 프레임워크를 제안한다. 마지막으로 5장에서 결론과 향후 연구 방향에 대해서 살펴본다.

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음(IITA-2007-C1090-0701-0026)

II. 관련 연구

2.1 Gaia

Gaia는 Illinois 대학에서 제안한 시스템으로 유비쿼터스 환경에서 사용자의 이동성을 지원하기 위해 시작되었다[2]. 여러 이동 단말들이 서로 작용하면서 등록되고, 사원들을 공유하고 서비스들끼리의 연계를 지원하는 시스템이다. 또한 디바이스끼리의 어플리케이션 개발을 지원하고 있다. 이러한 미들웨어를 설계하면서 이동성에 따른 인증은 구성하였지만 프라이버시에 대한 연구는 되지 않았다.

2.2 OpenID

OpenID는 개인의 신상 정보를 개인이 관리할 수 있는 분산형 공개 표준 기술이다[3]. 지금까지는 하나의 웹사이트에 로그인하려면 가입을 하고 개인의 신상정보를 해당 사이트에 넣어야 한다. 하지만 이 기술을 사용하면 개인이 하나의 URI 형태의 자신만의 아이디를 가지고 이를 이용하여 사이트에 로그인하게 된다. 또한 속성 교환 스펙을 이용하여 사용자의 개인 정보를 사용자가 허락하는 수준의 개인 정보만을 제공할 수 있도록 대화식 접근 방법을 사용한다. 그러나 개인의 인증 정보를 개인이 관리하도록 하고 있지만 그 후에 사용자의 행동에 대해서는 관리하지는 못한다.

2.3 OECD Guideline

"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"는 국제적 프라이버시 권고안이다[4]. 이 권고안에서는 개인의 정보를 수집할 때는 법을 지키고 정당한 이유가 존재할 때 수집해야 한다고 하고 있다. 수집한 정보에 대해서는 즉각적으로 알려야 하고 그 정보들은 위험이나 손실 없이 제한된 접근만 허용해야라는 보안을 지켜야 한다. 또한 자신의 정보에 대해서는 자신이 지우거나 제한하고, 고칠 수 있어야 한다[5]. 현재의 사회에서 부족한 부분의 개인 정보를 지우거나 제한할 수 있는 것이다. 개인이 행동한 내용을 서비스 제공자는 기록으로 남기지만 어느 정도의 기록으로 남기는지에 대해서 사용자에게 알려주지 않는 문제점도 있다.

III. 유비쿼터스에서의 프라이버시

유비쿼터스 환경에서의 프라이버시는 기존의 사회에서의 프라이버시와는 구분되어야 한다. 기존의 사회 통념상의 프라이버시는 개인의 식별이나 주소, 전화번호와 같은 개인을 식별할 수 있는 정보를 의미했다. 따라서 서비스 제공자는 개인 정보를 어떻게 저장하여 보호할 것인지에 대한 대응책을 연구하였다. 따라서 개인 정보를 암호화하고 개인 정보에 접근하는 권한을 제한하는 방법을 사용하였다.

유비쿼터스 환경에서의 프라이버시는 기존의 프라이버시 개념에서 자신의 위치 정보나 활동에 대한 정보와 기록등도 포함시켜야 한다. 사용자가 이동하는 경로가 여러 센서들을 통해서 연속적으로 파악될 수 있다. 현재는 어떤 도메인에서 어떠한 행동을 하였는가가 해당 도메인에 저장되게 된다. 이렇게 저장된 정보는 기존의 시스템과 같은 방법을 통해서 관리할 수도 있지만 서비스 제공자가 악의적인 목적으로 해당 정보를 유출하거나 허용되지 않은 공격자에 의해서 유출될 수도 있다. 이렇게 될 경우 기존의 개인 정보가 유출된 경우보다 심각한 문제가 발생한다. 한 개인의 일거수일투족이 낱낱이 공개되어 개인의 사회생활 자체를 위협할 수 있게 된다.

개인이 스스로 프라이버시를 관리해 나가야 하는 프라이버시를 나누어보면 다음과 같다.

- 개인을 파악할 수 있는 신상 정보
- 개인은 인지하나 그 안에서의 행동에 대한 정보

신자의 경우에는 지금까지 인증과 관련된 여러 연구들이 있다. OpenID가 대표적으로 Web 2.0 시대에 자신의 인증 정보를 자신이 관리할

수 있도록 하여 개인 정보를 보호할 수 있다. 하지만 추가에 대한 정보는 관리되지 못하고 있다. 예를 들어 사용자가 영화관에서 카드를 사용하여 영화를 결제하였다. 이때 영화관에서는 과금을 위하여 개인 정보와 결제에 관한 정보를 수집하여야 한다. 하지만 개인의 실할 과 학을 위하여 그 영화에 대한 정보를 수집할 수도 있는 것이다. 이 경우 사용자에 따라서 그러한 정보 수집을 불쾌하게 느낄 수도 있다. 이러한 것을 방지할 필요성이 있는 것이다.

Ⅳ. 프라이버시 관리 프레임워크

기존의 유비쿼터스에서 프라이버시를 지원하는 프레임워크에서는 사용자가 요청하는 서비스를 제공하고 그에 따른 접근 기록 또한 서비스 제공자가 관리하였다. 따라서 본 논문에서는 개인의 접근 기록 및 행동에 관한 기록을 개인이 관리할 수 있는 프레임워크를 제안한다. 도메인간의 인증과 서비스 요청에 대한 기본 구조는 "프라이버시 보호를 위한 동적 접근 제어 시스템"을 따른다[6]. 이 시스템은 홈 인증 서버를 두고 외부의 다른 도메인으로 이동하였을 때 해당 도메인과 동적인 협상을 통하여 사용자의 접근 제어를 지원하는 시스템이다. 사용자는 이동한 도메인의 도메인 관리자와 통신하여 인증하도록 한다. 이 환경에서 사용자는 서비스를 요청하고 그에 따른 접근 기록 등을 기록하는 시스템 구조는 다음과 같다.

그림 1. 시스템 구조도

사용자는 도메인 관리자에게 서비스를 요청한다. 이때 자신의 접근 정보를 관리할 보안 관리자의 접근 주소와 정보도 함께 제공하도록 한다. 이동한 도메인의 보안 관리자는 자신이 필수적으로 기록을 하여야하는 정보는 자신이 저장하고 그 외의 부가적인 정보들은 사용자의 홈 보안 관리자를 통하여 사용자가 직접 관리할 수 있는 기록 관리자에게 전달한다.

서비스 제공자가 보관하여야 하는 개인 정보는 서비스를 제공함에 있어서 해당 사용자를 관별할 수 있는 최소의 정보와 과금을 위한 금액 정도로 최소화해야 한다. 또한 보안 관리를 위한 정보등도 포함하여야 한다.

홈 보안 관리자에게 전달해야하는 정보는 다음과 같다.

- 서비스 제공자 정보
- 서비스 제공 컨텍스 내용
- 서비스 제공자가 기록한 정보 내용
- 서비스 제공자가 필요로 하는 부가 정보 내용

서비스 제공자는 위와 같은 정보를 사용자의 보안 관리자에게 전달하게 되면 서비스 제공자는 부가적인 정보에 대한 관리의 의무에서 벗어날 수 있는 장점이 있다. 그리고 만약 서비스 제공자가 해당 정보를 사용자로부터 제공받고 싶으면 자신의 기록 관리자로부터 사용자의 기록 관리자의 정보를 확인하여 원하는 정보를 요청한다. 사용자는 해당 요청에 대하여 선택적으로 정보를 제공한다. 미리 정의한 수준의 정보를 요청하는 서비스 제공자에게 제공하거나 미리 정의 되지 않은 내용을 요청할 때는 사용자의 허락을 요청하도록 한다. 또는 서비스 제공자와의 신뢰관계를 바탕으로 정보를 제공한다.

Ⅴ. 결론 및 향후 연구

본 논문에서는 개인의 프라이버시를 적극적으로 보호하기 위하여 개의 활동에 대한 기록 정보를 관리할 수 있는 시스템을 제안하였다.

제안한 프레임워크를 이용하면 서비스 제공자는 자신이 관리해야하는 정보의 양이 줄어들게 되고 관리에 따르는 비용을 절감할 수 있다. 또한 사용자는 자신의 정보를 직접 관리하게 되어 자신이 원치 않는 정보의 유출을 막을 수 있다.

향후에는 여러 서비스 제공자들을 파악하고 프라이버시를 보호를 지원하는 접근 기록 시스템으로 통합이 필요하다. 통합을 위해서 통합된 접근 기록 데이터 구조를 설계하여야 한다. 또한 개인의 접근 기록을 관리하는 서비스나 편리한 관리 도구를 개발할 필요가 있다.

[참고문헌]

[1] E. Gustafsson and A. Jonsson, "Always best connected," IEEE Wireless Communicaton., Vol. 10, no. 1, pp.49-55, Feb. 2003

[2] M. Roman et al, "Gaia: A Middleware Infrastructure to Enable Active Spaces," IEEE Pervasive Computing, pp. 74-83, Oct-Dec. 2002

[3] OpenID, http://openid.net

[4] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_119820_1_1_1,00.html

[5] M.Yasujiro, "Legal Issues for Realizing Ubiquitous Information Society," SICE Annual Conference 2004, pp1751-1754, Aug. 2004

[6] 이세훈, 김상욱, "유비쿼터스 환경에서 프라이버시 보호를 위한 동적 접근 제어 시스템", 정보과학회 추계학술발표대회, 2005