유비쿼터스 컴퓨팅 환경을 위한 프라이버시 빌딩 블록

고양우° 이동만
한국정보통신대학교
{newcat°, dlee}@icu.ac.kr

Privacy building block for ubiquitous computing environment

YangWoo Ko° Dongman Lee
School of Engineering, Information and Communications University

요 약

프라이버시의 보호는 유비쿼터스 컴퓨팅이 제기하는 중요한 이슈 중의 하나이다. 프라이버시 이슈의 해결에는 하나의 기술이 아니라 다양한 필요를 충족시키는 다양한 기술이 필요하다. 이 논문에서는 프라이버시 보호를 위하여 필요한 여러 가지 빌딩 블록 중에서 두 가지를 제안한다. 첫째 빌딩 블록은 사용자간의 상호 협력에 있어서 프라이버시 노출을 막아 주는 기능을 제공하며, 둘째 빌딩 블록은 사용자가 다른 사용자 또는 서비스와 대화함에 있어 허용되는 범위를 공간적으로 정의할 수 있도록 하는 기능을 제공 한다.

1. 서론

유비쿼터스 컴퓨팅의 가장 중요한 목표는 서비스가 어디에나 널리 존재하도록 하는 것과 환경 속에 자연스레 섞이어서 사용자에게 드러나지 않게 하는 것이다.[1] 이러한 환경은 당연히 많은 센서와 감지된 결과나 처리된 결과를 저장하는 기억장치로 가득 하게 되며 이는 기억 증폭 효과를 일으킨다. 이러한 특징 때문에 유니쿼터스 컴퓨팅 환경은 프라이버시 관점에서 심각한 이슈를 제기 하게 된다.[2]

프라이버시에는 다양한 정의가 있지만 "나에 대한 어떤 정보가 누구에게 알려질 것인지를 선택할 권리"라는 정의가 이 논문이 다루려는 대상과 대체로 일치한다. 유비쿼터스 컴퓨팅 기술에서 프라이버시는 필요에 의하여 추가되는 기능이 아니라 설계 단계에서부터 포함될 필요가 있으며 고려하여야 할 프라이버시의 측면에 대하여는 [2]에서 다음과 같이 여섯 가지를 제시하였다: (1) 고지(notice) (2) 선택과 동의(choice and consent) (3) 익명과 가명의 사용(anonymity and pseudonymity) (4) 근접성과 지역성(proximity and locality) (5) 보안(security) (6) 접근과 자원(access and resource)

이들 원칙 중에서 이 논문에서는 익명성과 근접성이라는 측면에서 프라이버시 보호를 지원하는 빌딩 블록을 제안한다. 익명성이라는 것은 자신의 실체를 드러내지 않으면서 서비스를 이용할 수 있는 방법을 의미하며 근접성은 사용자가 가까이에 있을 때만 그 사용자와 결부된 서비스가 가동되게 하는 것을 의미한다.

2. 사적 협력을 지원하는 빌딩 블록

유비쿼터스 환경에서의 컴퓨팅 모델에 대한 연구는 사용자와 그를 둘러싸고 있는 환경과의 대화를 중심으로 되어 있다. 하지만 실생활에서는 사용자들은 필요에 따라 사용자들 끼리 자원을 주고받으면서 협력하므로 유비쿼터스 환경은 이를 원활히 지원하여야 한다.

2.1 기존 연구와 문제 도출

협력을 지원하기 위해서는 한 사용자에게 부여된 권한을 다른 사용자에게 위임할 수 있어야 한다. [3]에서는 사용자들 간의 권한 위임을 잘 정의하고 있으나 반드시 제삼자의 확인을 통하여 위임하도록 되어 있어 사적인 협력의 프라이버시를 보호할 수 없다. [4]에서는 제삼자의 개입 없이 위임은 가능하지만 권한의 일부만 위임할 수 없다는 단점이 있다. 한편, [5]에서는 권한의 제어를 제삼자의 개입 없이 지원하는 방안을 제시하였지만 권한의 위임은 지원하지 못한다.

이 장에서는 *권한의 위임 과정에서 프라이버시의 노출을 최소화 함으로써 사적인 상호 협력을 가능하게 하는 빌딩 블록*을 제시한다. 상호 인증은 [5]에서 제시한 기법을 따르며 표기법도 같은 논문의 방식을 따랐다.

2.2 설계를 위한 가정

- 하나의 믿을 수 있고 안전한 권한 관리 서버가 존재한다. (이하 이 서버를 *L* 이라고 부른다. 이는 사용자가 어떤 서비스 환경으로 들어오기 위하여 로비에서 필요한 절차를 밟는다는 시나리오로부터 유래한 것이다.)
- 각 사용자는 자기의 신분을 증명하는 신분증(credential)을 받기 위하여 최소한 한번 *L*과 접촉한다.
- 각 서비스는 자기 자신을 등록하고 공유된 암호(shared secret)를 생성하기 위하여 *L*과 미리 접촉한다.

2.3 요구 사항

이 빌딩 블록은 다음과 같은 요구 사항을 만족시켜야 한다.

- 공유의 비밀 유지 : 한 사용자가 다른 사용자에게 자기의 권한을 양도하는 경우 *L*이 간여하지 않거나 또는 간여하더라도 누가 누구에게 무엇을 제공하려는 것인지 알 수 없어야 한다.
- 오프라인 상호 신뢰 : 사용자간 또는 사용자와 서비스간의 상호 인증은 *L*의 간여 없이 가능하여야 한다. 이는 서비스 이용 단계에서의 프라이버시 보호를 위하여 필요하다.
- 일시 양도와 영구 양도 : 권한은 제공자의 결정에 따라 일시적

으로 또는 영구히 양도 될 수 있어야 한다.

2.4 구현

일시 양도는 양도의 상황을 기록하는 토큰을 이용하여 구현하며 영구 양도는 은닉 서명(blind signature)을 이용하여 구현한다. 아래의 작동 예시 설명은 다음과 같은 가장 간단한 시나리오에 적용한 결과를 보여주는 것이다.

2.4.1 시나리오

사용자 A와 B는 서로 신뢰하며 서로의 공개키를 알고 있다. 사용자 A가 서비스 X를 사용하고자 하는데 접근 권한이 없다. 이때, 서비스 X에 대한 접근 권한을 가진 사용자 B가 A를 도와주려고 한다.

2.4.2 일시 양도

(1) A가 B에게 양도 요청을 보낸다. 이때 보내는 내용은 $\{\{X, nonce\}S_A\}P_B$ 가 된다. 여기서 nonce는 다른 사용자에 의한 되풀이 공격(replay attack)을 피하기 위하여 필요하다. S_A 와 P_B는 각각 A의 비밀키와 B의 공개키를 나타내며 중괄호로 묶은 내용을 그 키를 이용하여 암호화 한다는 것을 표시한다.

(2) B는 X에게 자신의 신분증을 보낸다. 신분증은 (V,b,P_B,Sig)로 구성된다. 여기서, V와 b는 비밀 집합(secret set)을 이용하여 B가 서비스 X에 대한 사용 권한을 갖고 있음을 입증하기 위하여 사용된다. (이에 대한 자세한 설명은 [5]를 참조) 한편, Sig는 이 신분증이 진짜로 L이 서명한 것임을 확인할 수 있도록 하는 값이다.

(3) 서비스 X는 B에게 자신의 인증서를 보낸다. 인증서는 X의 공개키를 L이 자신의 서명키로 암호화 한 것이다.

(4) B가 X에게 양도용 토큰을 요구한다. 이 요구에는 되풀이 공격을 피하고 양도 기간을 지정하기위해 $\{nonce,timeout\}P_X$를 인자로 보낸다.

(5) 서비스 X는 난수 DT(delegation token)를 발생시켜서 저장하고 그 값을 B의 공개키로 암호화하여 B에게 전송한다. 이때부터, 정해진 양도기간 동안에는 누구든지 이 DT를 제시하면 서비스 X를 이용할 수 있다.

(6) B가 A에게 DT를 A의 공개키로 암호화하여 전달한다.

(7) A가 X에게 인증서를 요구하고 X는 A에게 인증서를 제시한다.

(8) A가 자신의 신분증과 X의 공개키로 암호화한 DT를 제시함으로써 A가 서비스 X에 대한 접근 권한을 얻게 된다.

2.4.3 영구 양도

(1) ~ (3) 위와 같다.

(4) B가 서비스 X에게 $\{nonce,C_A\}P_X$를 보냄으로써 영구 양도를 요청한다.

(5) X는 B의 V 벡터의 X번째 비트를 $1-MSB(\{b_B\}K_X)$ 로 만들고 A의 V 벡터의 X번째 비트를 $MSB(\{b_A\}K_X)$ 로 만든다.

(6) 수정된 벡터를 이용하여 A와 B의 신분증을 새로 생성한다. 이 과정에서 은닉 서명을 함으로써 L은 새로 생성되는 신분증의 내용을 보지 않고 서명하게 된다.

(7) X가 A와 B에게 새로운 신분증을 전송한다.

2.5 검증

이 절에서는 제시한 빌딩 블록이 2.3에서 제시한 요구 사항을 만족시키는지 검증한다.

임시 양도의 경우에는 아예 L이 간여하지 않고 영구 양도의 경우에도 L이 은닉 서명을 하므로 공유의 비밀이 유지 된다. 오프라인 상호 신뢰는 [5]에서와 마찬가지로 비밀 집합을 사용하여 실현된다. 그리고 서로 다른 두 가지의 기법을 사용하여 일시 양도와 영구 양도를 모두 지원한다.

3. 대화 범위의 공간적 제약을 지원하는 빌딩 블록

실생활의 많은 기제는 현재의 환경을 기준으로 설계되어 있다. 예를 들어, 비밀회의를 할 때 회의실 앞에 문지기를 두는 것은 그 방안으로 들어오지 못하면 그 회의의 내용을 듣고 볼 수 없다는 가정에 기초한다.

하지만, 유비쿼터스 컴퓨팅과 이의 기반이 되는 무선 통신 기술은 이러한 가정을 무너뜨리게 된다. 그러므로 유비쿼터스 환경에서의 보안과 프라이버시를 위해서는 새로운 기술 환경에 맞추어 이때까지의 기제를 변경하거나 또는 기술을 이때까지의 기제에 맞추어 동작하게 하여야 한다. 물론, 이 두 가지는 병행될 것이며 여기에서는 후자의 접근 방법을 따른다.

사람은 자신의 대화가 일정한 공간(즉, "내 주변")에서만 들린다는 기존의 심상 모델(mental model)에 익숙하다. 그러므로 유비쿼터스 환경에서의 대화도 이와 같은 모델을 따르면 기존의 프라이버시 기제를 쉽게 적용할 수 있다.

3.1 기존 연구와 문제 도출

위치 정보를 이용하여 접근을 통제하는 기법으로서 널리 인용되는 것은 Geo-encryption 기법이다.[6] 하지만 이 기법은 매우 견고한 GPS(Global Positioning System) 단말기를 전제로 하고 있는 것이어서 일반적으로 적용하기는 어렵다.

한편, [7]에서는 제한된 영역에만 전파될 수 있는 신호(예를 들어, 초음파)를 이용하여 같은 방에 있는 사람들끼리만 암호를 공유하게 하는 방법을 제시하였다. 이 방법은 논리적 공간(예를 들어 "같은 방")에 잘 적용된다는 장점이 있는 반면에 벽으로 둘러쳐진 공간에서만 적용가능 하다는 단점이 있다. 두 대 이상의 믿을 수 있는 장치가 무작위의 강도로 봉화(beacon)를 주기적으로 생성하게 하고 각 사용자가 수신한 강도 값을 위치 정보를 나타내는 서명으로 이용하는 방안도 제안되었다.[8]

이 두 가지 방법은 앞의 것에 비하여 적용이 비교적 쉽다는 장점이 있음에도 불구하고 여전히 임의의 공간을 기준으로 접근을 통제하는 방식은 제시하지 못한다. 이 장에서는 [8]의 기법을 확장하여 사용자가 *자기 주변의 일정한 공간 이내의 다른 사용자에게만 대화를 전달하도록 지원하는 빌딩 블록*을 제시한다.

3.2 요구 사항

- 위치 기반 인증 - 주변의 사용자 또는 서비스는 그들의 신분이 아니라 위치에 의하여 인증되어야 한다. 이때 위치의 정밀도는 "내 주변"이라는 심상 모델을 만족시켜야 한다.
- 위치 정보 진정성(authenticity) - 만약 자신의 위치 정보를 쉽게 조작할 수 있다면 주변에 있지 않으면서도 대화를

듣는 것이 가능해진다. 따라서 사용자나 서비스가 주장하는 위치가 진짜라는 것이 보장되어야 한다.

- 보안 채널 - 대화의 발신자와 그 주변의 수신자 사이에만 비밀키를 공유하여 발신자와 수신자 사이의 대화에 기밀성(confidentiality)이 보장되어야 한다.
- 위치 정보의 유출 방지 - 다른 사용자의 위치 정보를 가로챌 수 있다면 자신의 위치를 조작하는 것이 가능하므로 위치 정보의 송수신은 유출을 피할 수 있는 방식으로 이뤄져야 한다.

3.3 설계를 위한 가정

- 믿을 수 있고 안전한 권한 관리 서버 *L*이 존재한다.
- 모든 사용자와 *L*은 서로의 공개키를 알 수 있다.
- 두 개 이상의 봉화 서버가 있으며 이들은 *L*과 서로 신뢰하며 안전하게 통신할 수 있다.

3.4 구현

3.4.1 세션 키 생성 단계

이 빌딩 블록은 크게 세 개의 단계로 나뉘어서 실행된다. 첫째 단계는 세션 키를 생성하는 단계이다. 이 단계는 다음과 같은 과정으로 진행된다.

(1) 세션을 시작하고자 하는 송신자 *S*가 *L*에게 세션 키 생성을 요구한다. 이때, 인자로서 $\{LS(S), 범위, 현재시간\}P_L$ 을 보낸다. 여기서, *LS(S)*는 *S*가 가장 최근에 받은 위치 서명(즉, 봉화 서버에서 받은 신호 강도의 순서쌍)이며, 범위는 이번 세션에서 허용할 물리적 공간의 범위를 나타낸다. 현재시간은 되풀이 공격을 막기 위한 것이다.

(2) *L*은 세션 식별자와 세션 키를 생성하여 이를 *S*의 공개키로 암호화 하여 *S*에게 준다. 이때, 세션 키는 대칭 키로 구현된다.

(3) *L*은 세션 식별자, 세션 키, 세션의 물리적 범위, 기간 등을 기록하여 둔다.

3.4.2 대화 진행 단계

하나의 세션이 초기화 되었으므로 대화가 진행되는 둘째 단계를 시작할 수 있다.

(1) 송신자 *S*는 자신이 보내고자 하는 자료를 세션 키로 암호화 하고 여기에 세션 식별자를 암호화되지 않은 형태로 덧붙여 보낸다.

(2) 주변의 다른 사용자들이 메시지를 받고 세션 식별자로부터 새로운 세션이 시작되었음을 알게 된다. 받은 자료를 풀기 위하여 수신자 *R*은 *L*에게 세션 키를 요구한다. 이때 보내는 인자는 $\{세션\ 식별자, LS(R)\}P_L$ 이 된다.

(3) *L*은 세션 키 요청에 대하여 요청하는 사용자들의 위치 서명과 저장된 세션 정보를 비교하여 조건이 만족되는 경우(즉, 송신자의 "주변에 있는" 수신자가 요청한 경우)에 대하여 세션 키를 수신자의 공개키로 암호화하여 전달한다.

(4) *R*이 세션 키를 받으면 그 세션의 모든 수신 정보를 해독할 수 있다.

3.4.3 세션 키 갱신

유비쿼터스 환경에서 사용자들은 움직인다. 이는 현재 진행되는 세션에 두 가지 이슈를 야기한다. 우선, 사용자들이 움직이기 때문에 "내 주변"의 의미가 계속 바뀐다. 따라서 주기적으로 새로운 세션 키를 생성하고 이를 "현재 송신자 주변"의 수신자들에게 전달하여야 한다. 또 하나의 이슈는 세션 정보 관리의 안정성이다. *L*이 관리하고 있는 세션 정보에 대하여 송신자가 명시적으로 세션의 종료를 알려주지 못하고 연결이 끊어질 수도 있으므로 각 세션 정보는 일정한 시간이 지난 후에 세션 키가 갱신되지 않으면 해당 세션 정보는 자동으로 폐기된다.

세션 키의 갱신은 주기적으로 이뤄지는 것이 일반적이지만, 송신자가 갑자기 많은 거리를 이동한 경우 송신자의 요청에 의하여 이뤄질 수도 있다. 세션 키의 갱신은 세션 생성과 근본적으로 같으므로 절차에 대한 설명은 생략한다.

3.5 검증

이 절에서는 제시한 빌딩 블록이 3.2에서 제시한 요구 사항을 만족시키는지 검증한다.

각 사용자가 자신의 위치 서명을 제시하고 봉화 서버의 신호 강도를 정확히 알 수 있는 제삼의 권한 관리 서버가 이를 확인함으로써 위치에 기반한 인증이 구현된다. [8]에서 이미 제시된 바와 같이 사용자는 봉화 서버를 구분할 수 없으므로 위치 서명을 조작할 수 없고 따라서 위치 정보의 진정성이 확보된다. 실제 대화는 송신자와 수신자가 공유하는 공유키를 이용한 보안 채널을 통하여 교환되며 위치 서명을 보낼 때 권한 관리 서버의 공개키로 암호화하므로 다른 사용자에게 위치 서명이 유출되지 않는다.

4. 결론

이 논문에서는 믿을 수 있는 제삼자와 공개키 알고리즘, 비밀 집합, 은닉 서명 등을 적절히 활용함으로써 프라이버시를 보장하면서 사용자간의 상호 협력이나 대화를 진행할 수 있도록 지원하는 빌딩 블록을 제시하였다.

참고문헌

[1] Deborah Estrin and others, "Connecting the Physical World with Pervasive Networks," IEEE Pervasive Computing, Volume 1, Number 1, Pages 59-69, Jan/Mar 2002.

[2] Marc Langheinrich, "Privacy by Design Principles of Privacy-Aware Ubiquitous Systems," In Proceedings of UbiComp 2001:International Conference on Ubiquitous Computing, Pages 273-291, 2001.

[3] Jeffrey Undercoffer and others, "A Secure Infrastructure for Service Discovery and Access in Pervasive Computing," Mobile Networks and Applications, Volume 8, Issue 2, Pages 113-125, April 2003.

[4] Jiejun Kong and others, "ESCORT: A Decentralized and Localized Access Control System for Mobile Wireless Acces to Secured Domains," Proceedings of the 2003 ACM Workshop on Wireless security, Pages 51-60, 2003.

[5] Kan Zhang and Tim Kindberg, "An Authorization Infrastructure for Nomadic Computing," In Proceedings of the seventh ACM Symposium on Access control models and technologies, Pages 107-113, June 2002.

[6] Dorothy E. Denning and Peter F. MacDoran, "Location-Based Authentication: Grounding Cyberspace for Better Security," In Computer Fraud & Security, Elsevier Science Ltd., February 1996.

[7] Tim Kindberg and Kan Zhang, "Context Authentication Using Constrained Channels," HP Labs Tech. Report HPL-2001-84, April 2001.

[8] Suman Banerjee and Arunesh Mishra, "Secure Spaces: Location-based Secure Wireless Group Communications," ACM SIGMOBILE Moble Computing and Communications Review, Volume 7, Issue 1, Pages 68-70, January 2003.