情 報 保 護 學 會 誌
第20卷 第4號, 2010. 8

신뢰 협상 기술 동향

김 영 삼*, 진 승 헌**

요 약

인터넷, 모바일 등을 이용한 서비스들이 다양한 개인정보를 이용하기 시작하면서, 사용자의 프라이버시 문제는 점점 더 심각해지고 있다. 이러한 프라이버시 문제를 해결하기 위해 여러 가지 연구가 진행되고 있으며, 그 중 하나가 신뢰협상(Trust Negotiation) 기술이다. 이 기술은 사용자의 데이터 노출제어 및 서비스제공자의 자원인가 및 제어간의 균형점을 찾아주어 사용자의 프라이버시 보호 및 서비스제공자의 접근제어를 가능하게 할 수 있다. 본 논문에서는 이러한 신뢰협상 기술 중 몇 가지를 살펴봄으로써 신뢰 협상 기술의 연구 동향 및 발전 방향에 대해 알아보고자 하였다.

Ⅰ. 서 론

기업네트워크와 같은 인트라넷에서는 자원에 대한 인가(Authorization)문제가 큰 보안이슈 중에 하나이다. 각 직원들마다 가지고 있는 보안레벨이 다르고 그에 따라 취급할 수 있는 자원 및 서비스가 다르기 때문이다. 초기의 접근제어(Access Control)기술은 이것을 가능하게 하였다. 각 직원들의 보안레벨(role)을 정의하고 그에 맞는 자원 및 서비스만을 사용할 수 있도록 함으로써, 기업의 보안성을 향상시키고 감사(Audit)를 용이하게 하였다. 이러한 접근제어기술이 오픈네트워크인 인터넷에 적용, 발전된 것이 신뢰협상기술이다. 인터넷은 기업네트워크와는 달리 자원요청자(requester)들이 일반적인 사용자이기 때문에, 자원을 적절히 인가하기 위해 사용자의 개인정보가 수집되며 이는 사용자의 프라이버시와 밀접한 관련이 있다. 또한 비대면이기 때문에 정보제공에 대한 계약서(약관)나 그에 대한 확인 과정이 허술하며 이는 사용자가 자신의 권익을 스스로 버리게 될 가능성을 내포하고 있다. 이에 따라 사용자 스스로 자신의 정보를 통제하는 자기정보통제권이라는 권리가 강조되기 시작하였고, 이는 새로운 접근제어기술인 신뢰협상 기술에 힘을 실어주고 있다. 본 논문에서는 이러한 신뢰협상 기술의 연구 동향을 살펴봄으로써, 신뢰협상 기술의 발전 방향을 가늠해본다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는, 신뢰협상 기술의 등장과정을 살펴보고, 3장에서는 이러한 신뢰협상 기술들이 어떻게 연구되고 있는가를 조사하고 분석하며, 마지막으로 4장에서는 향후 신뢰협상기술의 발전방향과 함께 결론을 내도록 한다.

Ⅱ. 신뢰협상 기술의 등장 배경

신뢰협상 기술은 접근제어기술의 한 형태라고 할 수 있다. 접근제어 기술은 ID 기반, role 기반, attribute 기반으로 나누어 볼 수 있는데, 이들은 모두 자원관리자(controller)가 알고 있는 사용자(previously known user)를 가정한다. ID기반 접근제어는 가장 간단한 형태의 접근제어로써, 보통 id/password 방식의 사용자 인증을 통해 사용자에게 자원이용에 대한 권한을 인가해주게 된다. 이 방식은 자원별 권한을 세분화할 수 없다는 점에서 보안상 많은 문제점이 발생할 수 있다. 이러한 문제점을 해결하기 위해 나타난 것이 RBAC (Role-Base Access Control)이다. RBAC는 자원관리자가 자원요청자를 분류할 특정 role을 생성하고, 그들에게 적절한 role을 부여한다. 각 role은 그에 맞게 접근가능한 자원이 매핑되어 있어 좀 더 세밀한 인가정책을 구현할 수 있다. 하지만 role은 모든 자원요청자들을 고려할 수 없기 때문에 인터넷 환경의 사용자들에게 적용

* 과학기술연합대학원대학교 정보보호공학과(kim03@etri.re.kr)
** 한국전자통신연구원 인증기술연구팀(jinsh@etri.re.kr)

하기에는 적절하지 못하다. RBAC가 coarse-grained 접근제어라고 하면, ABAC(Attribute-Base Access Control)는 fine-grained 접근제어라고 할 수 있다. ABAC는 자원요청자가 가지고 있는 속성(attribute)에 기반하여 그에 맞는 자원을 인가해준다.

이렇게 접근제어기술은 좀 더 세밀한 자원인가를 가능하게 하는 방향으로 발전해 왔지만, 분명 한계가 있다. 첫째, 중앙집중형 구조를 취하고 있다는 점이다. 이에 따라 기업과 같은 폐쇄된 도메인에서만 적용이 용이하며, 인터넷과 같은 오픈된 환경에서는 자원관리자의 비대칭적 정보공유로 인한 프라이버시 침해의 소지가 있다. 둘째, previosuly known user를 대상으로 한다는 점이다. 자원관리자는 자원요청자의 정보를 가지고 있으며 role에 따라 또는 속성에 따라 자원을 인가해준다. 이는 사용자의 자기정보통제권을 침해할 수 있어 문제가 될 수 있다.

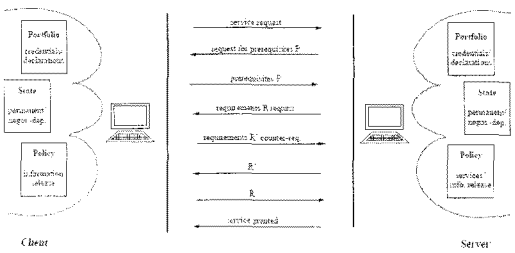
신뢰협상 기술은 이러한 문제점을 해결하려는 방향에서 등장하였다. 이 기술은 오픈 환경에서 stranger에게 어떻게 자원을 인가해줄 것인가를 목표로 하며, 사용자의 프라이버시 침해 요소를 최소한으로 하고, 정보의 대칭성을 최대화하는 방안을 제시한다. 신뢰협상 기술은 자원관리자와 자원요청자 사이에서 각각의 정책과 프로토콜에 따라서 인가가 이루어진다. 3장에서 우리는 이와 관련된 연구들을 살펴보도록 한다.

Ⅲ. 신뢰협상 기술의 연구동향

3.1 PSPL(Portfolio and Service Protection Language)[1]

Bonatti와 Samarati가 제안한 신뢰협상 프레임워크이다. 자원요청자는 포트폴리오(Portfolio)라는 속성정보의 집합을 가지고 있으며 그것은 credential과 declaration으로 나뉘어진다. credential은 TTP로부터 인증받은 정보를 말하고, declaration은 TTP로부터 인증받지 않은 정보를 말한다. 자원요청자는 portfolio disclosure rules를 통해 자신의 정책을 세울 수 있으며, 그에 따라 자신의 정보를 노출한다. 자원관리자는 service accessibility rules라는 접근제어 정책을 가지고 있으며, 그에 따라 자원인가를 수행한다[그림 1].

PSPL의 신뢰협상 프로토콜을 보면 크게 prerequisit, requisite, facet rule의 세 가지 형태의 rule로 구성된다.



〔그림 1〕 PSPL의 협상 프로토콜

prerequiste rule은 자원을 인가하기 이전에 만족되어야 하는 필요조건들을 명시한다. 이를 통해 서버는 의미없는 정책노출을 방지할 수 있다. 예를 들어 기존에 서버에 등록된 사용자만을 자원인가 대상으로 하고 싶을 경우 prerequisite rule에 기존 등록된 사용자 여부를 확인하도록 하는 rule을 추가하여 등록되지 않은 사용자와는 협상자체를 진행하지 않을 수 있게 된다. 다음으로 requisite rule은 각 자원별로 필요한 credential이나 declaration들을 명시한다. rule의 가독성 향상 및 정책의 크기를 줄이기 위해 abbreviation rule도 정의가 가능하다. 마지막으로 facet rule은 특정 자원에 대한 부가적인 기능들에 대해 정의할 수 있다. 예를 들어 책을 파는데 협력업체의 고객에게는 할인을 해주고 싶을 경우 facet rule에 명시하면 된다.

이렇게 PSPL은 자원관리자와 자원요청자가 각각의 정책을 세우고 그것을 바탕으로 협상을 한다. 이를 통해 자원관리자는 stranger에게 세밀한 자원인가를 할 수 있으며, 자원요청자는 정보노출을 스스로 제어함으로써 프라이버시를 보호받을 수 있다.

3.2 TPL(Trust Policy Language)[2]

Herzburg, Mass 등이 제안한 신뢰협상 시스템이다. TPL은 크게 TPL과 DTPL(Definite TPL)의 두 가지 형태의 정책 언어로 구성된다. DTPL은 TPL의 부분집합으로써 TPL에서 negative rule을 제거한 것이다. 따라서 DTPL은 monotonic 속성을 갖는다.[3] 여기서 monotonic이란 크리덴셜의 노출이 증가할수록 인가받을 수 있는 자원도 증가하는 속성을 말한다. TPL은 negative rule을 허용함으로써 크리덴셜 노출의 증가가 반드시 인가받는 자원의 증가를 의미하진 않는다. TPL은 XML을 기반으로 하며 GROUP 태그, RULE 태그, INCLUSION 태그 등으로 구성된다[그림 2]. 먼

```
<GROUP NAME="Hospitals">
    <!---- hospital recommended by at least 2 hospitals ---->
<RULE>
   <INCLUSION ID="reco" TYPE="Recommendation"
FROM="hospitals" REPEAT="2" DEPTH="3">
   </INCLUSION>
</RULE>
</GROUP>
```

〔그림 2〕 TPL 정책 예

저 GROUP tag는 role을 정의하며 하나이상의 RULE tag로 구성된다. RULE tag는 GROUP에 참여하기 위한 인증서의 집합을 정의한다. RULE tag는 하나이상의 INCLUSION tag를 가지고 있는데, 이INCLUSION tag는 다시 ID, FROM, TYPE, REPEAT, DEPTH 속성을 갖는다. ID는 인증서의 식별자로써, FUNCTION tag와 연결되어 해당 인증서에 대한 추가 제약사항을 명시할 수 있도록 한다. FROM은 issuer의 이름이며, TYPE은 인증서의 종류, REPEAT는 해당 GROUP에 속하기 위해 필요한 서로 다른 issuer의 인증서의 최소 개수, 그리고 DEPTH는 허용하는 최대 인증서 체인 길이를 의미한다. 추가적으로 FUNCTION tag는 앞서 언급하였듯이 특정 인증서에 대한 추가적인 제약사항을 명시하며, 이는 인증서가 가진 field에 의존적이다.

TPL은 신뢰협상보다는 기존의 접근제어에 더 가깝다고 할 수 있다. TPL은 인증서 기반의 RBAC를 나타내고 있기 때문이다. 따라서 구현 역시 서버쪽에 Add-on되는 형태이며, 이 Add-on모듈은 Certificate Library라는 개념을 통해 서로 다른 인증서라도 하나의 추상인증서 객체로 변환하여 쉽게 이용할 수 있도록 한다. TPL은 사용자 측면에서의 정책은 고려하지 않았기 때문에 실질적인 신뢰협상 기술이라고 하기는 어렵지만, 접근제어의 관점에서 인증서 및 인증서 체인을 XML기반의 정책으로 표현할 수 있도록 하여 stranger에 대한 접근제어를 가능하게 하였다는데 의의가 있다고 하겠다.

3.4 Trust-X[4]

Bertino, Ferrari, Squicciarini가 제안한 신뢰협상 프레임워크이다. Trust-X는 크게 X-TNL[5]이라는 XML 기반의 정책언어와, 협상 프로토콜로 나누어 볼 수 있다. 참고로 Trust-X에서 말하는 인증서는 PSPL의 portfolio와 같은 개념으로써 credential과 declaration으로 구성되며, 일반적인 공개키 인증서는 아니다.

$$
\begin{aligned}
pol_1 = (\{\}, & Rental\_Car \leftarrow Corrier\_Employee \\
& (code = Rental\_Car.requesterCode, \\
& position = driver), Id\_Card \\
& (name = Corrier\_Employee.name));\\
pol_2 = (\{\}, & Rental\_Car \leftarrow Driving\_Licence \\
& (name = Rental\_Car.name, issuer = EU));\\
pol_3 = (\{pol_2\}, & Rental\_Car \leftarrow Credit\_Card \\
& (name = Rental\_Car.nameRental\_Car.ReturnDate \\
& < ExpirationDate));\\
pol_4 = (\{pol_3, pol_1\}, & Rental\_Car \leftarrow DELIV).
\end{aligned}
$$

〔그림 3〕 disclsure policy 예

Trust-X는 disclosure policy라는 정책[그림 3]을 정의하며, 이는 여러개의 term으로 구성된다. term은 서비스나 인증서를 나타내며, 각각에 대한 접근제어 정책을 명시할 수 있다. 또한 disclosure policy는 pol_prec_set이라는 부분을 통해 단계적인 협상을 가능하도록 하였다.

협상 과정은 크게 intorductory, sequence generation, policy evaluation, certificate exchange의 네 단계로 나누어 볼 수 있다. 먼저 introductory 단계는 PSPL의 prerequisite rule과 같은 역할을 한다. 또한 이때 trust ticket이라는 것을 교환하게 되는데, 이는 협상의 속도를 향상시킬 수 있다. trust ticket은 자원관리자와 자원요청자 사이에 과거에 성공적인 협상이 있었다는 증표로써, 자원관리자의 서명이 검증되고, 만료일이 지나지 않았다면, 협상과정 없이 자원인가가 이루어질 수 있도록 하여 중복협상으로 인한 시간소모를 줄일 수 있도록 하였다.

두 번째 단계인 sequence generation 단계에서는 sequece predication module이 해당 자원관리자에 맞는 인증서 sequence를 예상하여 제공함으로써, 협상을 빠르게 할 수 있도록 한다. 이는 trust ticket과 같은 목적이지만 사용범위가 다르다. 즉 trust ticket은 특정 자원관리자에게만 사용가능하지만, sequece prediction module에서 생성한 sequence는 여러 자원관리자에게 사용할 수 있다. 이것이 가능한 이유는 자원관리자가 다르더라도 인가하려는 자원의 종류가 같다면 요구하는 인증서도 비슷할 수 있기 때문이다.

Trust ticket교환이나 sequece generation 단계에서도 협상이 완료되지 못했다면, 새로운 협상이 필요하다는 의미이므로 policy evaluation 단계를 진행한다. 이 단계에서는 자원관리자와 자원요청자 각각의 discolsure policy에 따라 협상이 진행되며 그 과정은 tree 형태로

저장된다. 협상은 서로의 정책을 단계적으로 노출하면서 진행하게 되는데, 하나의 자원에 대한 협상이라도 다양한 협상결과가 나올 수 있다. 이를 "협상전략의 다양화"라고 말하는데, 예를 들면 자원관리자가 나이를 알고 싶을 경우 면허증을 요구할 수도 있고, 주민증을 요구할 수도 있으며 declaration을 요구할 수도 있다. 이렇듯 협상전략의 다양화를 통해 나온 여러 개의 협상 결과를 Valid View라고 부르며 이에 따라 실제로 인증서를 교환하게 된다. 그리고 최종적으로 원하는 서비스를 인가받게 된다.

Trust-X는 P2P환경을 가정하며 신뢰협상의 전 과정을 구현하였다는 데에 큰 의미가 있다. 또한 trust ticket, sequence prediction module, negotiation tree등을 통해 다양한 협상 및 효율적인 협상을 가능하게 했다는 것에도 의미를 둘 수 있을 것이다.

3.5 FAMTN(Federated attribute management and trust negotiation)[6]

Spantzel, Squicciarini, Bertino가 제안한 Federation 환경에서의 신뢰협상 프레임워크이다. 이는 기존의 IdM의 한 형태인 Federation 모델에서의 협상 효율을 높일 수 있는 방안을 제시하였다. Trust-X와 마찬가지로 특정 자원관리자에 대해서 같은 자원에 대한 중복협상을 방지하기 위해 session ticket을 사용한다. 또한 협상이 성공하고 나면 그에 대한 trust ticket을 발행한다. 여기서의 trust ticket은 Trust-X의 그것과는 의미가 다르다. trust ticket은 자원요청자가 현재까지 이용한 자원의 목록이다. Federation 환경에서는 CoT(Circle of Trust)내에서 각 자원관리자간의 신뢰를 가정하므로, 서로간의 인증서 공유가 가능하다. 따라서 사용자는 협상 시 제공해야 하는 개인정보 중 일부를 직접적으로 제공하지 않고 session ticket을 제공함으로써, CoT내의 다른 자원관리자와 협상 시 사용했던 개인정보를 직접 제공하는 수고를 덜 수 있다. 이처럼 FAMTN은 신뢰협상을 특정 IdM모델의 특징을 이용하여 효율적으로 할 수 있다는 것을 보여준 데 의의가 있다.

Ⅳ. 결 론

인터넷 환경에서의 개인정보 제공은 서비스를 제공받기 위해 필수적인 것이지만, 그에 따른 프라이버시 문제도 만만치 않아, 계속 문제가 되고 있다. 본 논문에서는 이를 해결하기 위한 여러 방법 중 하나인 신뢰협상 기술의 동향에 대해 알아보았다. 지금까지 알아본 신뢰협상 기술들은 기존의 접근제어에 비해 복잡한 방법이기 때문에, 기업이나 사용자 모두 받아들이기 어려울 수 있으며, 사용성의 저하에 따른 보안성의 포기 현상을 야기할 수 있는 문제점이 있다. 현재까지는 이 기술이 실질적으로 적용된 사례를 찾아보기 힘들지만, 지속적인 연구를 통해 문제점을 개선해나간다면 사용자의 프라이버시를 보호할 수 있는 새로운 접근제어 기술로 자리매김할 수 있을 것이다.

참 고 문 헌

[1] Piero Bonatti, and Pierangela Samarati, "Regulating Service Access and Information Release on the Web," ACM Conference on Computer and Communications Security, Athens, Greece, pp. 134-143, Nov. 2000.

[2] Amir Herzberg, Yosi Mass, Joris Michaeli, Dalit Naor, and Yiftach Ravid, "Access Control Meets Public Key Infrastucture, Or: Assigning Roles to Strangers," IEEE Symposium on Security and Privacy, Oakland, CA, pp. 2-14, May. 2000.

[3] Kent E. Seamons et. al, "Requirements for Policy Languages for Trust Negotiation," Proceedings of the 3rd International Workshop on Policies for Distributed Systems and Networks, pp. 68-79, Jun. 2002.

[4] Elisa Bertino, Elena Ferrari, Anna Cinzia Squicciarini, "Trust-X: A Peer-to-Peer Framework for Trust Establishment," IEEE Transactions on Knowledge and Data engineering, Vol. 16, No. 7, pp. 827-842, Jul. 2004.

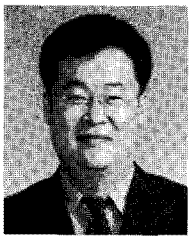
[5] E. Bertino, E. Ferrari, A. Squicciarini, "X-TNL: An XML-based Language for Trust Negotiations," Proceedings of the 4th International Workshop on Policies for Distributed Systems and Networks, pp. 1-4. Jun. 2003.

[6] Abhilasha Bhargavspantzel, Anna C. Squicciarini, Elisa Bertino, "Trust Negotiation in Identity Management," IEEE Security and Privacy, Vol. 5, pp. 55-63, Mar-Apr. 2007.

〈著者紹介〉

김 영 삼 (Youngsam, Kim)
학생회원

2009년 2월 : 충북대학교 컴퓨터공학과 졸업
2009년 3월 ~현재 : 과학기술연합대학원(UST) 석사과정
<관심분야> 정보보호



진 승 헌 (Seunghun, Jin)
정회원

1993년 2월 : 숭실대학교 전산학과 졸업
1995년 2월 : 숭실대학교 전산학 석사
2004년 2월 : 충남대학교 전산학 박사
1999년 ~ 현재 : 한국전자통신연구원 인증기술연구팀 팀장
<관심분야> PKI, 프라이버시, 정보보호