S-P3P: P3P 표준을 반영한 보안 프로토콜 설계 및 분석

최 현 우[†] · 장 현 수[††] · 고 광 선[†††] · 김 구 수[††††] · 엄 영 익[†††††]

요 약

P3P는 웹 서비스 제공자와 사용자 사이에서 사용되는 개인정보의 정의, 전송, 수집, 그리고 유지 등에 대한 정책을 정의하고 협상하기 위한 표준이다. 현재까지 제시된 P3P 표준은 주로 사용자의 개인정보보호 정책과 웹 서버의 P3P 정책을 정의하고 두 정책을 비교하는 방법을 제공하고 있다. 그러나 사용자와 웹 서버 사이의 개인정보 및 데이터의 안전한 전송을 위한 세부 기능과 이 때 발생할 수 있는 문제점에 대해서는 명확하게 제시하고 있지 않다. 이러한 문제점을 해결하기 위해서, 본 논문에서는 Secure P3P(S-P3P) 프로토콜을 제안한다. 제안 프로토콜은 현재의 P3P 표준을 위한 보안 프로토콜로서 웹 서버와 사용자 간의 상호 인증 기능을 제공하고, 전송되는 메시지와 데이터의 무결성과 기밀성을 보장한다. 또한, S-P3P 프로토콜은 사용자로부터 웹 서버에 전송되는 개인정보의 송수신에 대한 부인방지 기능을 제공한다.

키워드 : P3P, 개인정보보호, 상호인증, 보안프로토콜, 웹보안

Design and Analysis of a Secure Protocol for the P3P Standard

Hyunwoo Choi[†] · Hyun-Su Jang[††] · Kwang Sun Ko[†††] · Gu Su Kim[††††] · Young Ik Eom[†††††]

ABSTRACT

P3P(Platform for Privacy Preference) that is used in the World Wide Web is a standard to define and negotiate policies about definition, transmission, collection, and maintenance of personal information. Current P3P standard provides methods that define client personal information protection policy and P3P policy associated with web server. It also provides a method that compares these two policies. The current P3P standard, however, does not handle detail functions for safe transmission of the personal information and data. Also, it does not handle problems that can be induced by the detail functions. In this paper, in order to solve these problems, we propose a Secure P3P(S-P3P) protocol, which is a security protocol for the current P3P standard, offers mutual authentication between the web server and the client, and guarantees integrity and confidentiality of the messages and data. Furthermore, a S-P3P protocol provides non-repudiation on transmission and reception of personal information that is transmitted from the client to the web server.

Key Words : Platform for Privacy Preference(P3P), Privacy Protection, Mutual Authentication, Secure Protocol, Web Security

1. 서 론

웹을 기반으로 한 서비스의 공급과 수요는 산업, 연구 분야 및 개인사용 등의 다양한 분야에서 크게 증가하였다. 또한, 각종 조사에서는 향후 웹 서비스 시장이 더욱 성장할 것이라고 예측하고 있다[1]. 그러나 웹 서비스 이용 시에 사용자는 자신의 개인정보 노출 수준과 웹 서버에 의한 개인정보의 수집 및 저장, 그리고 이용에 대해서 정확히 알 수 없다. 이러한 단점은 웹 서비스 시장의 성장을 저해하는 중요한 요인으로 여겨지고 있으며[2], 개인정보보호를 위한 기술적, 정책적 문제는 시급히 해결해야 할 중요한 문제가 되었다.

Platform for Privacy Preference(P3P)는 웹 서비스 환경에서 개인정보의 정의, 전송, 수집, 유지에 관련된 웹 서버 측의 P3P 정책을 정의하고, 정의된 P3P 정책과 사용자의 개인정보보호 정책과의 협상 과정을 제시하고 있는 표준으로써, 웹 서비스 환경에서 개인정보의 정당한 수집과 보호 문제를 해결하기 위해 World Wide Web Consortium(W3C)를 통해 제안되었다[3-5]. 현재의 P3P 표준은 사용자가 명시적으로 확인할 수 있는 P3P 정책의 표현 방법과 비교 방법을 제공하는 것에 초점을 맞추고 있는 반면, P3P 정책 제공자인 웹 서버와 사용자 사이의 정책 협상 과정을 위한 세부적인 기술적 절차나 그

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음.(IITA-2007-(C1090-0701-0046))
† 준 회 원 : 성균관대학교 대학원 전기전자컴퓨터공학부 석사과정
†† 준 회 원 : 성균관대학교 대학원 전기전자및컴퓨터공학과 박사과정
††† 정 회 원 : 성균관대학교 대학원 이동통신공학과 연구교수
†††† 정 회 원 : 동양대학교 정보통신공학부 교수
††††† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2007년 6월 27일, 심사완료 : 2007년 10월 15일

요구사항은 명시하지 않고 있다[6, 7]. 신뢰할 수 있는 두 객체 간의 안전한 통신 방법을 제공하는 것은 웹 기반의 서비스 제공 환경에서는 반드시 필요한 기능으로서, P3P 표준 Specification 1.1에서는 앞으로 개발될 표준 P3P 프로토콜이 포함해야 하는 이러한 기능을 추상적으로 제시하고 있다[8, 9]. 따라서 본 논문에서는 웹 서버와 사용자 사이의 상호인증 기능을 제공하고, P3P 정책 협상 과정에서 전송되는 메시지와 주요 데이터에 대한 무결성과 기밀성을 보장하며, P3P 정책 협상 결과에 따라 전송되는 사용자 개인정보에 대해, 사용자 측의 개인정보 전송에 대한 부인을 방지하는 기능과 웹 서버 측의 사용자 개인정보 수신에 대한 부인방지[10] 기능을 제공하는 Secure P3P(S-P3P) 프로토콜을 제안한다. 제안된 프로토콜을 이용함으로써 P3P Specification 1.1에서 제시하고 있는 웹 서버와 사용자 사이의 인증 기능을 제공하고, P3P 정책 협상 과정에서 전송되는 데이터를 안전하게 보호하며 개인정보의 제공과 수집에 대한 부인을 방지 할 수 있다.

SSL/TLS는 웹 서비스 이용 시 인증을 수행하고 보안 통신을 위한 협상과정을 제공하는 보안 프로토콜로서[11, 12], 전자 상거래 등 보안이 요구되는 웹 서비스에 널리 사용되고 있다. SSL/TLS 프로토콜은 주로 전자 상거래 시에 웹 서버 인증과 대칭키를 이용한 암호통신에 사용되고 있다. 이와는 다르게 P3P를 위한 협상 프로토콜은 사용자의 개인정보를 웹 서버에 안전하게 전송하는 것과 더블어 전송된 개인정보의 송신 및 수신 사실을 명확하게 입증할 수 있는 메커니즘을 제공해야 한다. 즉, SSL/TLS 프로토콜은 사용자에 대한 인증을 생략하거나 인증서 요구와 같은 간단한 방법을 사용하는 반면, P3P를 위한 협상 프로토콜은 사용자를 분명하게 인증하는 것과 동시에, 개인정보의 송신 및 수신에 대한 사용자와 웹 서버의 부인을 방지할 수 있는 메커니즘을 제공해야 한다. 이와 같은 기능은 웹 서버에 의해 수집된 개인정보의 저장과 추가적인 활용 등을 위해서 반드시 요구되는 기능이라고 할 수 있다. 또한, 웹 서버는 동시에 여러 웹 서비스를 제공할 수 있으며 각 웹 서비스에 대한 P3P 정책 파일이 별도로 존재하기 때문에 사용자가 여러 웹 서비스를 이용하기 위해서는 특정 P3P 정책과 자신의 개인정보보호정책을 비교하는 협상 과정을 반복 수행해야 한다. 물론 이러한 과정에서도 전송되는 개인정보에 대한 송신 및 수신에 대한 부인 방지 메커니즘이 동일하게 요구된다. 이러한 기능적 측면에서 본 논문에서 제안하는 보안 프로토콜은 전송 메시지의 무결성과 기밀성 제공에 초점을 맞춘 웹 서비스를 위한 보안 통신 프로토콜에 비해 P3P 협상에 적합하게 구성되었다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 현재의 P3P 표준을 살펴보고 확장된 P3P 프로토콜이 제공해야 하는 기능에 대한 요구 사항을 정리한다. 3장에서는 2장의 요구 사항을 바탕으로 본 논문이 제안하는 Secure P3P 프로토콜 설계를 위한 주요 가정 및 용어와 프로토콜의 세부적인 동작 과정과 특징을 설명하고, 4장에서는 메시지 무결성 및 기밀성, 웹 서버와 사용자 사이의 상호인증 그리고 개인정보 송신 및 수신에 대한 부인방지 기능과 같은 제안 프로토콜이 제공하는 핵심적인 기능에 대한 검증을 수행한다. 마지막으로, 5장에서 본 논문의 제안 기법을 정리하고 논문을 마친다.

2. P3P

본 장에서는 W3C에 의해 제안된 P3P 표준의 개요와 그 프로토콜 수행 절차에 대해 설명한다. 아울러 최근의 P3P 표준 문서인 P3P specification 1.1에 제시된 P3P 표준의 확장 기능으로부터 본 논문에서 제안하고 있는 보안 프로토콜의 필요성과 그 요구사항을 도출한다.

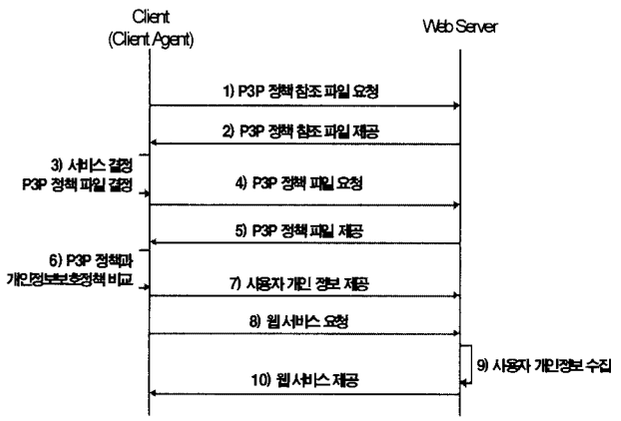
2.1 P3P 표준 분석

웹 환경에서 서비스를 제공하는 웹 서버는 그 서비스를 이용하는 사용자의 개인정보 수집에 대한 정책을 P3P 표준에 따라 정의한다. 사용자는 P3P 표준에 따라 정의된 웹 서버의 P3P 정책과 자신의 개인정보보호 정책의 비교를 통하여 웹 서버가 제공하는 서비스의 이용여부를 결정할 수 있다. 현재 AT&T에서 개발한 Privacy Bird[13], 마이크로소프트의 Internet Explorer 6.0(IE 6.0)[14], Netscape 네비게이터 7.0 버전 등이 P3P 또는 이와 유사한 기능을 지원하고 있다. 이러한 기능을 제공하기 위한 현재의 P3P 표준은 다음 <표 1>과 같은 요소들을 정의하고 있다[9]. P3P 정책 파일은 웹 서버가 제공하는 특정 서비스가 요구하는 개인정보의 정의, 수집 목적, 종류 그리고 수집된 개인정보의 이용 방법 및 저장과 관리에 대한 정책을 정의하며, P3P 정책 참조 파일은 각 서비스에 해당하는 P3P 정책 파일의 위치를 담고 있다. 사용자는 P3P 표준에 따라 자신의 개인정보보호 정책을 정의하고 편집할 수 있으며, 사용자 에이전트는 웹 서버의 P3P 정책과 사용자의 개인정보보호 정책을 비교하고 협상하는 과정을 수행한다. 이러한 과정을 거쳐 사용자는 자신의 개인정보를 웹 서버에 제공하고 웹 서버가 제공하는 서비스를 이용할 수 있다.

(그림 1)은 P3P 표준에 제시된 표준 프로토콜의 수행 절차

〈표 1〉 P3P 프로토콜의 참여 주체별 구성 요소

참여 주체	구성 요소 정의
웹 서버	P3P 정책 참조 파일(P3P Policy Reference File)
	P3P 정책 파일(P3P Policy File)
사용자 시스템	사용자 에이전트(Client Agent)
	사용자 개인정보보호 정책(Personal Information Protection Policy)
	사용자 개인정보(User Privacy Information)



(그림 1) P3P 표준 프로토콜 세부절차

를 보인다. 표준 P3P 프로토콜의 세부 과정은 (그림 1)에 보인 순서에 따라 이루어진다.

2.2 P3P 보안 프로토콜 요구사항

최근의 P3P 표준 문서인 P3P Specification 1.1에서는 다음 버전의 P3P 표준 프로토콜이 포함해야 할 확장된 메커니즘을 다음 <표 2>에서와 같이 제시하고 있다. 그러나 현재의 P3P 표준은 이러한 프로토콜 수행에 필요한 구체적인 기능과 그 요구사항은 정의하고 있지 않다.

<표 2>에서 보인 바와 같이 P3P Specification 1.1에서 제시하고 있는 확장 메커니즘은 기능적인 측면에서 크게 두 가지 기능으로 다시 구분할 수 있다. 첫 번째는 사용자가 웹 서버의 P3P 정책과 자신의 개인정보보호 정책을 명확하게 비교 할 수 있게 하기 위하여 P3P 정책을 정의하고 비교하는 방법을 제공하는 것이다. 두 번째는 웹 서버와 사용자 사이에 전송되는 데이터를 보호하는 등 구체적인 통신 방법을 제공하는 것으로 본 논문에서 제안하는 P3P 보안 프로토콜은 위의 두 가지 기능 중 주로 두 번째 기능을 제공하는 것에 초점을 맞추고 있다. 이것은 P3P Specification 1.1에서 제시하고 있는 <표 2>의 네 가지 확장 메커니즘 중 Ⅲ, Ⅳ번에 해당하는 기능이다.

P3P Specification 1.1에서 제시하고 있는 P3P 프로토콜의 확장 기능을 바탕으로 본 논문이 제안하는 P3P 보안 프로토콜이 제공해야 할 기능적 요구 사항을 정리하면 다음 <표 3>과 같다. 본 논문에서는 P3P Specification 1.1에서 제시한 위와 같은 확장 메커니즘과 이러한 기능을 제공하기 위한 요구 사항을 기반으로 P3P 보안 프로토콜을 설계하였다.

3. Secure P3P 프로토콜

본 장에서는 2장에서 제시한 요구 사항을 반영한 P3P 보안 프로토콜인 Secure-P3P(S-P3P) 프로토콜 설계에 필요한 주요 가정 사항 및 용어를 정의하고 S-P3P 프로토콜의 동작 과정에 대해 설명한다.

<표 2> P3P Specification 1.1에 제시된 확장 메커니즘

순서	메커니즘 설명
Ⅰ	웹 서버가 사용자에게 P3P 정책의 선택을 제공할 수 있도록 하는 메커니즘
Ⅱ	사용자 에이전트를 통하여 사용자가 웹 서버의 P3P 정책에 명확한 동의를 할 수 있는 메커니즘
Ⅲ	웹 서버와 사용자 사이의 협상 동의에 대한 부인을 방지하기 위한 메커니즘
Ⅳ	사용자가 자신의 개인정보를 웹 서버에 전송하기 위한 메커니즘

<표 3> Secure P3P 프로토콜 요구사항

요구조건	설명
메시지 무결성	공격자에 의해 메시지가 임의로 변경되지 않았음을 보장
메시지 기밀성	전송 메시지를 암호화하여 공격자에 의한 메시지 확인을 불가능하게 함
상호인증	웹 서버와 사용자 사이의 상호인증 기능
송신 부인방지	사용자가 웹 서버의 P3P 정책에 대한 동의에 의해 자신의 개인정보를 발송했음을 증명함
수신 부인방지	사용자가 송신한 개인정보를 웹 서버가 올바로 수신하였음을 증명함

3.1 가정 및 용어 정의

다음은 2장에서 설명한 기능을 제공하는 S-P3P 프로토콜 설계를 위한 주요 가정 사항이다.

- 개인키는 소유자를 식별할 수 있는 유일한 키이며, 키 소유자의 서명을 생성함
- 인증서는 신뢰할 수 있는 인증기관에 의해 발급됨
- 안전성이 검증된 단방향 해시함수, 공개키 기반 메시지 암호화, 대칭키 기반 메시지 암호화 기법을 웹 브라우저를 통해 지원함
- 웹 서비스 사용자는 웹 서버의 P3P 정책과 자신의 개인정보보호 정책을 비교하여 개인정보 제공 여부를 결정함

본 논문에서 제안하는 S-P3P 프로토콜은 전송 메시지의 무결성 및 기밀성, 프로토콜을 구성하는 두 객체 사이의 상호인증 그리고 프로토콜 과정에서 전송되는 주요 데이터의 송수신에 대한 부인을 방지하기 위한 기능을 제공한다. 다음 <표 4>는 S-P3P 프로토콜에 사용된 주요 용어의 정의를 보여 준다.

〈표 4〉 S-P3P 프로토콜 용어 정의

사용목적	용어	정의
표준 P3P 구성요소	PRF	P3P 정책 참조 파일 (P3P Policy Reference File)
	PPF	P3P 정책 파일(P3P Policy File)
	PPP	개인정보보호 정책 (Privacy Protection Policy)
	UPI	사용자 개인정보(User Privacy Information)
상호인증 구성요소	PU_i	i의 공개키
	PR_i	i의 개인키
	$E_{PR_i}(a)/D_{PU_i}(a)$	i의 개인키를 이용한 a에 대한 서명 생성/서명 검증
	$E_{PU_i}(a)/D_{PR_i}(a)$	i의 공개키를 이용한 a의 암호화/복호화
	$CERT_i$	i의 인증서
메시지 무결성 기밀성	$h(a)$	a에 대한 해시 코드 생성
	$E_{SK}(a)$	대칭키 SK를 이용한 a의 암호화
	$D_{SK}(a)$	대칭키 SK를 이용한 a의 복호화
	SK	대칭키
부인방지	RN_i	i에 의해 생성된 의사난수
사용자식별	UCN	사용자 식별 번호(Unique Client Number)
기타	$\|$	concatenation
	a/b	a와 b의 비교(comparison)

〈표 5〉 S-P3P 프로토콜 전체 과정

Step	Client	Transport data	Web Server	Step
0	*generate PRF request message*	$\{PRF\ request\ msg\} \rightarrow$	*processing the request*	1
		$\leftarrow \{PRF,\ CERT_S\}$		
2	*generate symmetric key* SK_1 $E_{SK_1} = E_{pk_S}(SK_1)$ $H_1 = h(PPF\ request\ msg \| E_{SK_1} \| SK_1)$	$\{PPF\ request\ msg,\ E_{SK_1},\ H_1\} \rightarrow$	$SK_1 = D_{PR_S}(E_{SK_1})$ H_1 *verification* *generate UCN* *generate* RN_S $E_{RN_S \| UCN} = E_{SK_1}(RN_S \| UCN)$ $H2 = h(PPF \| E_{RN_S \| UCN} \| RN_S)$	3
		$\leftarrow \{PPF,\ E_{RN_S \| UCN},\ H2\}$		
4	$(UCN,\ RN_S) = D_{SK_1}(E_{RN_S \| UCN})$ H_2 *verification* *comparison : PPP/PPF* *generate symmetric key* SK_2 $E_{UPI} = E_{SK_2}(UPI)$ $SIG_C = Sig_{PR_C}(RN_S \| E_{UPI})$ $H_3 = h(service\ request\ msg \| E_{UPI} \| UCN)$	$\{service\ request\ msg,\ E_{UPI},\ SIG_C,\ H_3\} \rightarrow$	H_3 *verification* SIG_C *verification* $SIG_S = Sig_{PR_S}(E_{UPI})$ *store* SIG_C	5
		$\leftarrow \{SIG_S\}$		
6	SIG_S *verification* $E_{SK_2} = E_{SK_1}(SK_2)$ *store* SIG_S	$\{E_{SK_2}\} \rightarrow$	$SK_2 = D_{SK_1}(E_{SK_2})$ $UPI = D_{SK_2}(E_{UPI})$	7
		$\leftarrow \{service\ response\}$		

3.2 초기 서비스 접근

다음 <표 5>는 본 논문이 제안하는 S-P3P 프로토콜의 전체 동작 흐름을 보여준다. S-P3P 프로토콜의 전체 동작 과정은 8단계로 이루어진다. S-P3P 프로토콜은 사용자가 웹 서비스를 이용하기 위해 웹 서버에 접근하여 웹 서버의 P3P 정책 참조 파일을 요청하면서 시작된다. 각 동작 과정의 세부 수행 절차는 다음과 같다.

Step 0. client 웹 서버에 PRF 요청 메시지 전송

Step 1. web server 사용자의 PRF 요청에 대해 PRF와 자신의 인증서를 전송

Step 2. client 대칭키 SK_1을 생성하여 웹 서버의 공개키로 SK_1에 대한 암호문을 생성
암호 코드와 PRF 요청 메시지 그리고 SK_C에 대한 해시 코드 생성

Step 3. web server 대칭키 SK_1을 획득하여 전송된 해시 코드를 검증
UCN과 RN_S를 생성하여 RN_S와 UCN을 SK_1으로 암호화
암호 코드 $E_{RNs||UCN}$과 PPF 그리고 RN_S 대한 해시 코드 생성

Step 4. client $E_{RNs||UCN}$을 복호화하여 UCN과 RN_S 획득
전송된 해시 코드를 검증하고 PPF와 PPP를 비교
대칭키 SK_2를 생성하여 자신의 개인정보를 암호화
RN_S와 암호화된 개인정보에 개인키로 전자 서명을 생성
웹 서비스 요청 메시지, 암호화된 개인정보, UCN에 대한 해시 코드 생성

Step 5. web server 전송된 해시 코드와 사용자의 전자 서명 검증
전송된 RN_S 검증
암호화되어 전송된 사용자 개인정보에 대하여 개인키로 전자 서명 생성
사용자의 서명 값 저장

Step 6. client 전송된 웹 서버의 전자 서명 검증
대칭키 SK_2를 SK_1으로 암호화
웹 서버의 서명 값 저장

Step 7. web server 전송된 암호문을 복호화하여 SK_2 획득
SK_2를 이용 암호화된 개인정보를 복호화하여 사용자의 개인정보 획득
사용자에게 웹 서비스 제공

다음 <표 6>은 사용자의 웹 서비스 초기 접근 시 S-P3P 프로토콜의 수행에 사용되는 암호화 및 복호화, 서명 그리고 해시 함수의 사용 횟수를 보여준다.

〈표 6〉 S-P3P 프로토콜에 사용된 서명의 생성 및 검증, 암호화 및 복호화 그리고 해시함수의 시행 횟수

수행 주체	서명 생성	서명 검증	공개키 암호화	개인키 복호화	대칭키 암호화	대칭키 복호화	해시 함수
사용자 시스템	1	1	1	0	2	1	2
웹서버	1	1	0	1	1	2	1

3.3 웹 서버 내의 다른 서비스 접근

웹 서버는 *Step 3*에서 사용자 식별을 위한 UCN을 생성하여 각 사용자에게 부여한다. UCN은 웹 서버에 서비스를 요청하는 각 사용자에게 부여되는 유일한 식별번호로, UCN을 사용하여 웹 서버는 각 사용자를 식별하게 된다. 웹 서버는 각 사용자에게 부여된 UCN에 따라

Client Key Information Table에 각 사용자의 인증서 정보와 대칭키 정보를 유지하며 이것들을 사용하여 프로토콜 상의 각 *Step*에서 필요한 암호화 및 복호화를 수행한다. 특히 *Step 7*을 마치고 웹 서버는 각 Client Key Information Table Entry의 대칭키 값을 마지막 복호화에 사용된 키 값(SK_2)으로 교체하여 사용자가 동일한 웹 서버가 제공하는 다른 서비스를 이용하고자 할 때의 P3P 협상과정에 사용한다.

다음 <표 7>은 웹 서버 측의 Client Key Information Table을 보여준다.

웹 서버는 동시에 여러 서비스를 운용할 수 있기 때문에 각 웹 서비스마다 요구되는 사용자의 개인정보가 다를 수 있으며, 이에 따라 웹 서비스 마다 서로 다른 P3P 정책 파일을 제공한다. 본 논문에서 제안하는 S-P3P 프로토콜에서 사용자는 동일한 웹 서버가 제공하는 다른 서비스를 이용하기 위해 UCN을 이용하여 <표 5>의 *Step 2* 시점에서부터 프로토콜 과정을 시작할 수 있다. 다음 <표 8>은 동일 서버가 제공하는 다른 서비스를 이용할 때의 프로토콜 과정을 보여준다. 나타낸 과정 *Step 2'*와 *Step 3'*는 <표 5>의 전체 프로토콜 수행 과정 중 *Step 2*와 *Step 3*을 대체하며 이후의 과정은 동일하다.

Step 2'. client
- 사용자 식별 번호 UCN을 SK_2로 암호화
- PPF 요청 메시지와 암화 코드 그리고 SK2를 이용해 해시 코드 생성

Step 3'. web server
- 해시 코드를 검증하고 UCN을 통해 사용자 식별

〈표 7〉 Client Key Information Table

UCN	대칭키	인증서
1	$SK_{client\,1}$	$CERT_{client\,1}$
2	$SK_{client\,2}$	$CERT_{client\,2}$
·	·	·
n	$SK_{client\,n}$	$CERT_{client\,n}$

〈표 8〉 동일 웹 서버의 다른 서비스를 이용 - Step 2와 Step 3 대체 프로토콜 수행 과정

Step	Client	Transport data	Web Server	Step
2'	$E_{SK_2} = E_{SK_2}(UCN)$ $H_1 = h(PPF request\ msg \| E_{SK_2} \| SK_2)$	$\{PPF request\ msg,\ E_{SK_2},\ H_1\}$ →	H_1 *verification* *check the UCN* *generate* RN_S $E_{RN_S} = E_{SK_2}(RN_S)$ $H_2 = h(PPF \| E_{RN_S} \| RN_S)$	**3'**
		← $\{PPF,\ E_{RN_S},\ H_2\}$		

• RN_S를 생성하여 SK_2로 암호화한 후, PPF, RN_S와 함께 해시 코드 생성

4. 보안 분석 및 검증

이번 장에서는 제안 프로토콜에서 제공하는 메시지 무결성 및 기밀성, 상호인증, 데이터 송수신 부인방지를 위한 프로토콜의 보안 기능을 검증한다. 보안 검증에는 다음 <표 9>에서 정의하는 용어와 3장의 <표 4>에서 정의한 용어를 사용한다.

〈표 9〉 S-P3P 프로토콜 보안 검증을 위한 용어 정의

용어	정의
$A \mapsto B$	객체 A로부터 B로의 메시지 전송
msg	전송 메시지(message)
X_A	공격자 X의 A로의 위장

4.1 메시지 무결성 및 기밀성

S-P3P 프로토콜은 프로토콜 수행 과정에서 전송되는 주요 메시지와 데이터에 대한 암호 코드와 해시 코드를 생성한다. 메시지 암호화는 대칭키를 이용하여 공개키 기반 암호화 방식에 비해 수행시간을 단축하고, 전자봉투 방식의 암호화를 한 차례 수행한다. 또한, 단방향 해시 함수를 사용하여 해시 코드를 생성한다.

(정리 1) S-P3P 프로토콜은 프로토콜 수행 과정에서 전송되는 메시지와 개인정보의 무결성과 기밀성을 보장한다.

(증명) 메시지 무결성 및 기밀성 보장

1. C : $\geq \neq rate\ symmetrickey\ SK_2$
   $E_{UPI} = E_{SK_2}(UPI)$
   $H_0 = h(service\ request\ msg \| E_{UPI} \| UCN)$
2. $C \mapsto S$: $\{service\ reqest\ msg,\ E_{UPI},\ H_0\}$
   if $attacker\ X\ intercept\ the\ msg\ from\ path\ 2$
2'. $X_C \mapsto S$: $\{service\ reqest\ msg',\ E_{UPI}',\ H_0'\}$
3. S : $H_1 = h(service\ request\ msg \| E_{UPI} \| UCN)$
   $comparison:\ H_0/H_1$
   $SIG_S = E_{PR_S}(E_{UPI})$
4. $S \mapsto C$: $\{SIG_S\}$
5. C : $E_{UPI}' = D_{PU_S}(SIG_S)$
   $comparison:\ E_{UPI}/E_{UPI}'$
   if $match$,
   $E_{SK_2} = E_{SK_1}(SK_2)$
   $where\ SK_1\ is\ symmetrickey\ that\ is\ already\ transmitted$
   if $attacker\ X\ transmits\ illegal\ message$
5'. C : $\because comparison:\ E_{UPI}/E_{UPI}'\ is\ failed$
6. $C \mapsto S$: $\{E_{SK_2}\}$
7. S : $SK_2 = D_{SK_1}(E_{SK_2})$
   $UPI = D_{SK_2}(E_{UPI})$

S-P3P 프로토콜에서 사용자는 전자봉투 방식을 사용해 대칭키를 웹 서버에 전송하고 이 대칭키를 이용해 이후의 통신을 수행한다. 암호방식의 안전성은 공개키 암호화 기법의 안전성에 기반하고 있으며, 전송된 대칭키와 대칭키를 이용해 암호화하여 전송한 비밀 값을 해시 코드에 포함하여 전송 메시지의 무결성을 보장한다.

4.2 상호인증

S-P3P 프로토콜은 사용자와 웹 서버 사이의 상호인증 기능을 제공한다. 사용자는 대칭키를 생성하여 웹 서버의 공개키로 암호화하여 웹 서버에 전송한다. 웹 서버는 자신의 개인키를 이용해 이를 복호화하여 대칭키를 획득할 수 있으며 이후의 프로토콜을 계속 수행할 수 있다. 이와는 다르게 웹 서버는 사용자의 전자 서명을 검증함으로써 사용자에 대한 인증을 수행한다.

(정리 2) S-P3P 프로토콜은 두 참여 객체 즉, 웹 서버와 사용자 사이에 상호인증 기능을 제공한다.

(증명) 웹 서버 인증

1. S : $processing\ PRF\ request\ msg$
2. $S \mapsto C$: $\{PRF,\ CERT_S\}$
3. C : $E_{SK_1} = E_{PU_S}(SK_1)$
   $SIG_C = E_{PR_C}(RN_S)$
4. $C \mapsto S$: $\{CERT_C,\ SIG_C\}$
5. S : $RN_S' = D_{PU_C}(SIG_C)$
   $comparison:\ RN_S'/RN_S$
   $\because$ if $match,\ dient\ authentication\ suceed$

사용자는 웹 서버의 공개키를 이용해 대칭키를 암호화해 전송하기 때문에 웹 서버가 그에 대응하는 정당한 개인키를 가지고 있지 않다면 이후의 협상과정을 지속할 수 없다.

(증명) 사용자 인증

1. S : $E_{RN_S \| UCN} = E_{SK_1}(RN_S \| UCN)$
   $where\ SK_1\ is\ symmetrickey\ that\ already\ transmitted$
2. $S \mapsto C$: $\{E_{RN_S \| UCN}\}$
3. C : $(RN_S,\ UCN) = D_{SK_1}(E_{RN_S \| UCN})$
   $SIG_C = E_{PR_C}(RN_S)$
4. $C \mapsto S$: $\{CERT_C,\ SIG_C\}$
5. S : $RN_S' = D_{PU_C}(SIG_C)$
   $comparison:\ RN_S'/RN_S$
   $\because$ if $match,\ dient\ authentication\ suceed$

사용자는 웹 서버로부터 수신한 의사 난수에 전자서명을 생성하여 웹 서버에 제공함으로써 자신이 공개키에 대응하는 개인키를 소유한 정당한 사용자임을 증명한다.

4.3 메시지 송수신 부인방지

S-P3P 프로토콜은 개인정보의 제공과 수집에 대한 과정을 정의한다. 따라서 P3P정책에 대한 동의에 의해 사용자가 자신의 개인정보를 웹 서버에 전송한 것과 웹 서버가 이 개인정보를 수신하였음을 증명할 수 있는 기능을 제공해야 한다.

(정리 3) S-P3P 프로토콜은 프로토콜 수행 결과에 따라 전송되는 사용자 개인정보의 송신과 수신에 대한 부인방지 기능을 제공한다.

(증명) 송신부인방지

---

1. S : *generate pseudo random number* RN_S
   generate unique client number UCN
   $E_{RN_S \| UCN} = E_{SK1}(RN_S \| UCN)$
   where SK_1 *is symmetric key that already agreed*
   $H_0 = h(PRF \| E_{RN_S \| UCN} \| RN_S)$
2. $S \mapsto C$: $\{PPF, E_{RN_S \| UCN}, H_0\}$
3. C : $(UCN, RN_S) = D_{SK_1}(E_{RN_S \| UCN})$
   $H_1 = h(PPF \| E_{RN_S \| UCN} \| UCN)$
   comparison: H_0 / H_1
   generate symmetric key SK_2
   $E_{UPI} = E_{SK_2}(UPI)$
   $SIG_C = E_{PR_C}(RN_S \| E_{UPI})$
4. $C \mapsto S$: $\{E_{UPI}, SIG_C\}$
5. S : $E_{UPI}' = D_{PU_C}(SIG_C)$
   comparison: E_{UPI} / E_{UPI}'
   store E_{UPI}, SIG_C

사용자는 암호화된 개인정보에 자신의 전자서명을 생성하여 웹 서버에 전송하고, 웹 서버는 이를 검증하여 보관함으로써 사용자가 자신의 개인정보를 전송하였음을 입증할 수 있다.

(증명) 수신부인방지

---

1. C : *generate symmetric key* SK_2
   $E_{UPI} = E_{SK_2}(UPI)$
2. $C \mapsto S$: $\{E_{UPI}, CERT_C\}$
3. S : $SIG_S = Sig_{PR_S}(E_{UPI})$
4. $S \mapsto C$: $\{SIG_S\}$
5. C : $E_{UPI}' = D_{PU_S}(SIG_S)$
   comparison: E_{UPI} / E_{UPI}'
   store SIG_S

$\because$ *result is matched* if and *only* if *when* S *has* E_{UPI}

웹 서버는 사용자로부터 수신한 암호화된 개인정보에 전자서명을 생성하여 전송하고, 이를 수신한 사용자는 그 전자서명을 검증함으로써 웹 서버의 개인정보 수신에 대한 부인을 방지할 수 있다.

5. 결 론

Platform for Privacy Preferences(P3P) 표준은 World Wide Web Consortium(W3C)에서 추진하고 있는 개인정보보호정책 표준으로, 웹을 통해 전송되어 사용되는 개인정보의 정의, 전송, 수집, 관리 등에 관계된 정책을 표현하고 협상하는 등, 웹 서비스 이용 시 발생할 수 있는 프라이버시 문제를 다루고 있다. 본 논문에서 P3P 프로토콜에 참여하는 두 객체 사이에서 개인정보의 안전한 전송 방법과 개인정보의 송신 및 수신에 대한 부인방지 기능을 포함하는 S-P3P 프로토콜을 제안했다. 제안된 S-P3P 프로토콜은 P3P 프로토콜을 구성하는 두 객체 사이의 상호인증을 제공하고, 단방향 해시함수를 이용한 해시 코드와 공개키 및 대칭키 암호화 방식을 이용한 암호문을 사용함으로써 웹 서버의 P3P 정책과 사용자의 개인정보보호 정책 협상 과정에서 전송되는 메시지와 데이터의 무결성과 기밀성을 보장하며, 개인정보의 전송과 수신에 대한 부인방지 기능을 제공할 수 있음을 보였다. 본 논문에서 제안한 S-P3P 프로토콜을 사용하여 P3P Specification 1.1에서 제시하고 있는 P3P 프로토콜의 확장 메커니즘을 구현할 수 있으며, 이를 통해 더욱 안전한 웹 서비스의 이용과 개인정보 제공 및 수집을 가능하게 하여 웹 서비스의 이용을 더욱 촉진할 것이다.

참 고 문 헌

[1] L. Aversano, G. Canfora, A. De Lucia, and P. Gallucci, "Intergrating Document and Workflow Management Tools using XML and Web Technologies: A Case Study", Proc. of Sixth European Conference of Software Maintenance and Reengineering, pp.24-33, 2002.

[2] M. S. Ackerman, "Privacy in pervasive environments: next generation labeling protocols", Personal and Ubiquitous Computing, Vol. 8, Issue 6, pp.430-439, 2004.

[3] L. Cranor, M. Langhinrich, and M. Marchiori, "A P3P Preference Exchange Language 1.0 (APPEL1.0)", W3C Working Draft, 2001.

[4] L. F. Cranor, "P3P: making privacy policies more useful", Security & Privacy Magazine, IEEE, Vol. 1, Issue 6, pp.50-55, 2003.

[5] Purpose of Platform for Privacy Preferences, http://en.wikipedia.org/wiki/P3P#Purpose.

[6] M. Bennicke and P. Langendorfer, "Towards automatic negotiation of privacy contracts for Internet services", Proc.

of 11th IEEE Conference on Computer Networks, ICON2003, IEEE Society, pp.319-324, 2003.

[7] L. Cranor, L. Marc, M. Massimo, P. Martin, and R. Joseph, "The Platform for Privacy Preferences 1.0 specification", http://www.w3.org/TR/P3P/, 2002.

[8] L. Cranor, H. Giles, L. Marc, M. Massimo, P. Martin, R. Joseph, and S. Matthias, "The Platform for Privacy Preferences 1.1 specification", http://www.w3.org/TR/P3P11/, 2006.

[9] H. Hochheiser, "The platform for privacy preference as a social protocol: An examination within the U.S. policy context", ACM Transactions on Internet Technology (TOIT), Vol. 2, Issue 4, pp.276-306, 2002.

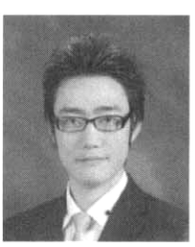
[10] W. Stallings, *Cryptography and network Security - Principles and Practices* (Fourth Edition)". PEARSON Education.

[11] A. O. Freier, P. Karlton and P. C. Kocher, "The SSL Protocol Version 3.0', Netscape, http://wp.netscape.com/eng/ssl3/draft302.txt, 1996.

[12] A. Elgohary, T. S. Sobh and M. Zaki, "Design of an enhancement for SSL/TLS protocols", Computers & Security, Elsevier, Vol. 25, Issue 4, pp.297-306, 2006.

[13] AT&T privacy bird, AT&T, http://www.privacybird.com, 2002.

[14] Privacy in Internet Explorer 6, http://msdn.microsoft.com/workshop/security/privacy/overview/privacyie6.asp, MICROSOFT.

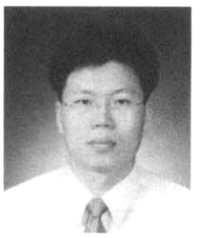


최 현 우

e-mail : iskraskk@ece.skku.ac.kr
2006년 성균관대학교 전기전자컴퓨터공학부(학사)
2006년~현재 성균관대학교 대학원 전기전자컴퓨터공학부(석사과정)
관심분야 : 모바일 에이전트, 네트워크 보안, 유비쿼터스 컴퓨팅

장 현 수

e-mail : jhs4071@ece.skku.ac.kr
2002년 성균관대학교 전기전자및컴퓨터공학과(학사)
2005년 성균관대학교 대학원 전기전자및컴퓨터공학과(공학석사)
2007년~현재 성균관대학교 대학원 전기전자및컴퓨터공학과(박사과정)
관심분야 : 유비쿼터스 컴퓨팅, 이동 에이전



고 광 선

e-mail : rillar91@ece.skku.ac.kr
1998년 성균관대학교 정보공학과(학사)
2004년 성균관대학교 대학원 전기전자및컴퓨터공학부(공학석사)
2007년 성균관대학교 대학원 전자전기컴퓨터공학과(공학박사)
2007년~현재 성균관대학교 대학원 이동통신공학과 연구교수
관심분야 : 정보보호, 리눅스, 네트워크 등

김 구 수

e-mail : gusukim@dyu.ac.kr
1994년 성균관대학교 정보공학과(학사)
1996년 성균관대학교 정보공학과 (공학석사)
2006년 성균관대학교 정보통신공학과 (공학박사)
2007년~현재 동양대학교 정보통신공학부 교수
관심분야 : 분산 컴퓨팅, 이동 에이전트 등

엄 영 익

e-mail : yieom@ece.skku.ac.kr
1983년 서울대학교 계산통계학과(학사)
1985년 서울대학교 전산과학과 (이학석사)
1991년 서울대학교 전산과학과 (이학박사)
2000년~2001년 Dept. of Info. and Comm. Science at UCI 방문교수
2005년 한국정보처리학회 학회지 편집위원장
1993년~현재 성균관대학교 정보통신공학부 교수
관심분야 : 분산 컴퓨팅, 이동 컴퓨팅, 이동 에이전트, 시스템 보안, 운영체제, 내장형 시스템 등