개인정보보호를 위한 안전한 다자계산 기술평가시스템*

성순화, 공은배
shsung@ce.cnu.ac.kr, keb@ce.cnu.ac.kr

Secure multiparty computation technology valuation system for privacy protection

Soon Hwa Sung, Eun Bae Kong
Dept. of Computer Engineering, Chungnam University
shsung@ce.cnu.ac.kr, keb@ce.cnu.ac.kr

요 약

인터넷의 발전으로 이동 전자상거래에서 개인 휴대단말기의 개인정보보호에 대한 필요성이 절실하다. 따라서 본연구는 개인 휴대단말기의 허가된 사용자를 나타내는 패스워드를 다자계산을 위한 PP(Proactive Pseudorandomness)protocol의 단일 패스워드체제로 해커에 능동적이며 신속하게 대처할 수 있으며, 제3의 인증기관없이 개인 휴대단말기의 허가된 사용자를 인증할 수 있다. 또한 개인정보보호를 위한 새로운 프로그램이 대체될 때, 그 대체프로그램의 효과를 기술평가시스템을 도입하여 증명가능 키분배의 영지식프로토콜로 기술 발전속도 변화의 사회적 영향을 검토할 수 있다.

1. 서 론

최근 인터넷 기술의 발달로 개인 휴대단말 이용자가 급증하면서 개인 휴대단말을 이용한 각종 경제활동이 활성화되면서 개인 정보이용에 관한 피해 사고가 빈번해지고 있다. 개인 정보는 정보사회에서 정보가 가치의 중심이 되고, 가치 있는 정보량에 따라 부를 창출할 수 있기 때문에 개인 정보량이 회사의 가치척도의 기준이 되는 세상이 되었다. 이로서 개인정보를 수집하려는 방법과 개인 정보의 수집 항목도 다양하다. 인터넷을 통해 수집되는 개인정보로 개인 정보 침해 뿐만 아니라 개인 정보 유출로 오.남용과 같은 금융사고 등의 사고가 빈번히 발생하고 있다. 이에 맞선 프라이버시 보호기술에는 중요한 문제점을 내재하고 있는데 그 기술 효과를 발휘하고 있는지 파악하기가 거의 불가능하다. 또한 침해당한 사실을 알아내어 수정작업이 기술적으로 제대로 된것인지 확인 역시 매우 어려운 현실이다.

인터넷의 탄생과 사용배경은 분명 미래 우리 삶의 방향을 정확히 예측해 주었다. 그러나 인터넷의 현실적인 편익과 미래의 발전은 악의에 찬 hacker와 cracker에 의해 크게 위협받고 있다. 최근 미국의 아마존 웹사이트와 CNN, 야후에 대한 해커의 DoS(Denial of Service)공격으로 약 1조 4천억 정도의 경제적 손실을 입은 사례와 이메일로 유포되는 악성 바이러스(Virus)에 의한 정보손실은 비용산정조차 못할 천문학적 규모이다.

따라서 인터넷의 발전과 대중화가 가져온 가장 커다란 문제점 중 하나가 불법적인 해킹을 일삼는 해커의 양산이다. 인터넷의 긍정적인 면을 확대 발전시키려면 이를 방어하려는 정보보안 정책과 기술지원이 병행되어야 한다. 그러므로 본연구는 이동전자상거래에서 휴대단말기를 이용한 각종 경제활동으로 빚어진 개인정보 피해 사고를 줄이고자 PPprotocol을 위한 안전한 다자계산을 제시한다. 그리고 이 다자계산의 기술효과를 파악하고 대체기술 확인을 위한 기술평가시스템을 제안한다.

2. 증명가능 다자간 프로토콜

본연구는 이동전자상거래에서 사용자가 제시한 패스워드를 안전하게 보장할 수 있으며, 문제가 발생했을 때 제3의 인증기관없이 인가된 사용자를 증명할 수가 있다. 뿐만 아니라 이동전자상거래에서 해커된 프로그램을 대체할 수 있는 프로그램이 제시되었다면 그 프로그램의 효율성을 테스트할 수 있는 기술 평가시스템을 제시한다. 그 프로그램의 비밀성은 최대한 보장하면서 이동전자상거래에 미치는 영향 뿐만 아니라 사회 전반의 영향까지도 알아낼 수 있다. 이는 예상 가능한 영향의 확인, 특정 프로그램을 이행하는 대체 기술수단의 확인, 필요한 목표를 달성하기 위한 대체 프로그램 확인, 대체 기술 수단과 프로그램의 영향에 대한 측정과 비교등을 검토할 수 있다.

n명의 참가자 $p_1,p_2,\ldots,p_n$가 각각의 비밀정보 s_i를 가지고 있어서 각 P_i는 s_i를 비밀로 한 채 임의의 함수값$f(s_1,..,s_n)$을 알고 싶다고 할 때, 다자간 프로토콜은 신뢰할 만한 센

* 이 연구는 충남대학교 정보통신인력사업단의 RA 지원금에 의해 수행되었음

터를 사용하지 않고 $f(s_1,..,s_n)$의 값을 얻기 위해 $p_1,p_2,...,p_n$ 사이의 메시지를 주고 받는 규칙이다. 이는 영지식증명으로 반수미만의 P_i 의 집합 A는 어떠한 부정을 한다할 지라도 A이외의 P_j의 s_j 를 아는 것이 불가능함을 말하며(privacy), A가 어떠한 부정을 한다할지라도 임의

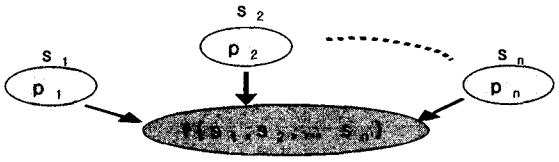

그림 1 다자간 프로토콜

의 P_j는 $f(s_1,..,s_n)$ 의 값을 알 수 있다(correctness). 기술평가시스템은 이동전자상거래의 사용자 패스워드를 PPprotocol로 전송받아 영지식증명으로 안전한 다자간 계산을 한다. 만약 대체프로그램이 실행된다면 효율성을 계산하기 위해 증명 가능 비밀분배로 Shamir의 secret sharing[1]을 사용한다. 즉 다자간프로토콜의 각 참가자의 비밀정보를 n개 분할해서 n명의 참가자에 분배한다. 이중 k명이 모이면 원래의 비밀을 복원할 수 있다. 이런 분배자는 자신의 비밀s를 상수항으로 하는 랜덤한 (k-1)차의 다항식 $f(x)$을 선택한다. $f(x)=s+a_1x+...+a_{k-1}x^{k-1} \bmod p$(p는 s<p인 소수). 분배자는 각 참가자 j(j=1,...,n)에 f(j)를 분배한다. n개의 분할된 정보 f(j)의 임의 (k-1)개의 분할정보로는 s를 분할할 수 없다. 그러나 k개 이상의 분할 정보를 이용하면 반드시 s를 복원할 수 있다.

3.다자계산을 위한 PPprotocol

현 개인 휴대단말 보안수준은 거의 서비스 업체가 가지고 있는 정보를 보호하는 수준으로 극히 개인적인 정보가 저장되어 있다. 이러한 개인 정보가 저장되어 있는 휴대단말의 분실시 완전히 제3자에게 정보가 공개될 수 있다. 현재 개인 정보 유출을 막기 위한 방법으로 단말 자체에서 비밀번호를 부여하여, 비밀번호를 모르면 정보를 열람하는데 어려움이 있으나 원천적으론 해결할 수 없다. 즉 4자리 숫자의 조합으로 4자리 숫자인 경우의 수는 10,000가지 경우로 암호자리수 증가로 경우의 수는 증가할 지 몰라도 원천적 보안이 될 수 없다. 따라서 본 연구는 사용자가 사용하는 이동전자상거래에서 휴대단말기의 사용자인증을 할 수 있게 하는 PP protocol을 제안한다.

암호는 외부의 악의있는 entities에 대해 상호작용하는 parties를 보호하는 것으로 insecure channels,

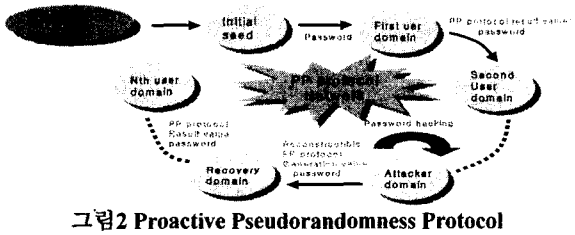

그림2 Proactive Pseudorandomness Protocol

인증파티들, unforgetable siganatures, and general multiparty secure computation에 대해 private communication을 가능케 한다. 만약 상대방이 protocol을 제어할 수 있다면 복구할 방법과 security를 다시 얻는 것이 불가능하다. 따라서 PPprotocol 설계는 Parties 계산의 시작에서만 randomness 를 사용하고, 한번 상호작용을 시작하면 더해진 randomness는 무효가 된다. 각round에서 그전round에서 오류가 발생한 party 일지라도 상대방이 예측할 수 없는 fresh pseudorandom number를 각 party에 공급한다.

이러한 pseudorandom numbers는 security를 다시 얻는 fresh random numbers로 party를 복구하는데 사용될 수 있다. Pseudorandom sequence는 같은 seed를 사용하여 다시 같은 sequence를 generate할 수 있다. 이러한 특성은 반복할 수 있는 시뮬레이션과 디버깅의 목적으로 유용하므로 PP protocol은 각 round의 각 party내 generate된 값이 그 party의 시작 계산값에 의해 선택된 seeds에만 의존한다. 이러한 값은 상대방에 의존해서는 아니되며, PP는 상대방이 엿들을 때에만 reconstructible 된다. 즉 입력 $x_1,...,x_n$을 가진 n parties $P_1,...,P_n$ 네트워크에서 Each input value x_i is uniformly distributed in {0,1}, where k is security parameter. Pseudorandom function family $F=\{f_k\}_{k\in\{0,1\}^k}$, where $f_k:\{0,1\}^k \rightarrow \{0,1\}^k$. 각 round l 에서 각 party P_i는 internal value(key) $k_{i,l}$를 계산한다. Round l에서 P_i 의 출력 $r_{i,l}$를 $r_{i,l}=f_{k_{i,l}}(0)$, where 0 is an arbitary fixed value으로 하고, 각 Round $l\geq 0$ 끝에서 party P_i 는 $f_{k_{i,l}}(j)$를 각 party P_j에 보낸다. 그런 후 P_i는 round l에 대한 key를 지우고 round $l+1$ 에 대한 key를 이 round의 모든 parties로부터 받은 값의 bitwise exclusive or로 설정한다. $K_{i,l+1}=\oplus_{j=1}^{n} f_{k_{j,l}}(i)$로 parties은 the old keys를 지운다. The parties의 initial inputs이 임의로 선택된다면 각 round의 각 party내에 generated value은 모든 round에서 모든 다른 paties 내에서 generate될지라도 상대방의 random과 구별할 수 없다. 이러한 protocol을 PP protocol이라고 한다[2].

4.개인정보보호를 위한 안전한 다자계산 기술평가시스템

본 연구는 이동전자상거래에서 이동단말기의 개인정보보호를 위해 개인 휴대단말기의 접근시 허가 받은자만이 이동전자상거래에 참여하는 프라이버시 보호를 위한 PP protocol을 제시하여 중립으로 그 프라이버시를 평가하는 시스템을 제시한다. 이 시스템은 다자계산기술과 그기술 프로그램이 현재 미치고 있는 영향, 또는 예상 가능한 영향의 확인, 특정 프로그램을 이행하는 대체 기술수단의 확인, 필요한 목표를 달성하기 위한 대체 프로그램 확인, 대체 기술수단과 프로그램의 영향에 대한 측정과 비교 등을 검토할 수 있다. 우선 PP protocol로 인증받은 사용자가 휴대 단말기에 접근할 수 있도록 Pseudorandom Number Generator[3]에서 유도된 psedorandom함수값을 initial seed로 한다. 휴대 단말기에는 initial seed를 입력으로 PP protocol의 출력을 키로 셋팅시킨다. 만약 상대방이 엿들을 때에는 reconstructible computation[4]이 되어 initial seed의 같은 sequence를 generate한 새로운 키

값으로 사용자 인증을 한다. 따라서 각 이동전자상거래의 사용자는 휴대단말기의 패스워드를 Pseudorandom Number Generator에서 유도된 psedorandom함수값을 initial seed로 한다. 그 패스워드를 입력으로한 PPprotocol의 출력을 쇼핑몰 진입시 패스워드가 되고, 이 패스워드를 입력으로한 PPprotocol의 출력을 지불시의 패스워드가 되며, 배송 역시 같은 방법으로 이루어진다. 만약 도중에 패스워드 해킹이 일어나면 reconstructible PPprotocol 로 새로운 키값을 생성하여 한번의 해킹으로 password체제가 무너지지 않는다. 사용자만이 key를 알고 제어하며 모든 이동전자상거래영역을 단일패스워드체제로 인증할 수 있다. 기술평가시스템에 PPprotocol로 전달된 n사용자의 비밀패스워드는 기술평가시스템에서는 내용을 모른채 그 패스워드가 안전하게 이동전자상거래에 적용이 되고 있다는 것을 영지식프로토콜로 증명을 할 수 있다. 만약 현재 프로그램을 대체할 수 있는 새로운 프로그램이 실행된다면 그 프로그램의 키로 효율성을 평가할 수 있는 증명가능 키분배의 영지식프로토콜로 확인할 수 있다.

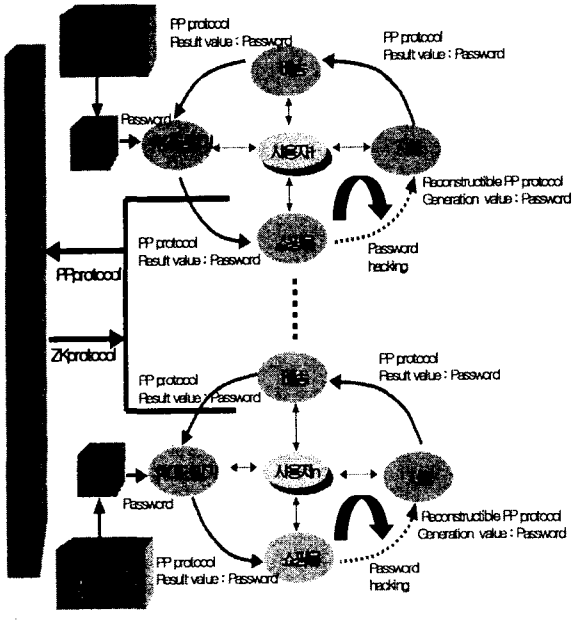

그림 3 안전한 다자계산 기술평가시스템

5.결론

본 연구는 이동전자상거래에서 휴대단말을 분실한 사용자, 휴대 전화 서비스 업체의 개인정보 해킹, 원격 개인 휴대단말 정보 해킹시 능동적이고 신속하게 처리할 수 있는 PPprotocol을 사용한 안전한 개인정보보호의 다자계산을 위한 기술 평가시스템을 제시한다. 이는 제3의 인증기관 없이 개인정보를 안전하게 인증관리할 수 있으며, 효율적 다자간계산으로 이동전자상거래에서의 단일사용자 패스워드메카니즘을 구성할 수 있다. 따라서 제3 인증기관에 투자하는 비용을 절약할 수 있으며, 또한 이동전자상거래에서의 사용자 패스워드관리에 드는 비용을 절감할 수 있다.

만일 이동전자상거래에서 개인보호를 위한 새로운 프로그램으로 대체할 수 있는 대체프로그램을 실행시킨다면 대체프로그램의 개인키로 그 프로그램이 현재 미치고 있는 영향, 예상가능한 영향 확인, 대체기술 수단 및 비교 검토등을 증명가능 키분배의 영지식프로토콜로 확인할 수 있다. 이로써 사회, 국가, 경제, 문화,교육등의 유대관계를 파악할 수 있으므로 기술문제를 기술문제로 극복하지 않는 계기가 마련된다. 그리고 전자상거래분야, ubiquitous computing, 정보가전의 안전성 보장, 컴퓨터시스템 신뢰성 제고, 다자계산의 안전성 보장등에 활용할 수 있다.
그러나 기술평가시스템과 사회, 국가, 경제, 문화,교육등의 유대관계를 어떻게 설계할 것인가의 과제가 남아 있다.

참고문헌

[1]A. Shamir. How to share a secret. Communications of the ACM, 22:612-613, November 1979

[2]Ran Canetti, "Studies in Secure Multiparty Computation and Applications", Thesis for the degree of Dr, pp. 131-134 ,1996

[3]http://cnscenter.future.co.kr/main/research/spring.html

[4]Ran Canetti, "Studies in Secure Multiparty Computation and Applications", Thesis for the degree of Dr, pp. 12-15 ,1996