Ad-hoc wireless network에서의 authentication을 보장하는 zero-knowledge proof 기반의 프로토콜

윤여원*, 예홍진

*아주대학교, 정보통신전문대학원

Zero-knowledge proof based authentication protocol in ad-hoc wireless network

Yeo-won Yoon*, Hong-Jin Yeh

*Graduate School of Information and Communication, Ajou University

요 약

본 논문에서는 ad-hoc wireless network에서 상호간의 사전지식 없이 상대편을 authenticate하는 프로토콜을 제시한다. 기존에 Dirk Balfanz et al에 의해 제시된 변형된 interactive Guy Fawkes protocol은 해쉬함수의, 전달하고자 하는 메시지와 그 authenticator의 해쉬값을 보내고, 다음 단계에서 그 원본을 밝히는 원리를 이용한 것으로, PKI 없이 해쉬함수 만으로 상호인증과 메시지의 무결성을 보장함으로써 전반적인 ID 체계와 public key encryption, decryption 연산에 대한 부담을 덜었다. 하지만, 이것은 여전히 eavesdropping같은 passive attack에 노출되어 있다[1]. 본 논문에서는 zero-knowledge 기반의 프로토콜을 이용하여 상호 정보를 교환할 수 없는 환경에서도 안전하게 상호 authentication을 가능하게 하는 방법을 제시한다.

I. 서론

1. Ad-hoc wireless network에서의 authentication 문제

1) Ad-hoc wireless network

Ad-hoc wireless network은 multihop radio network으로 서로 통신하고, 분산된 방식의 연결상태를 유지하는 자율적인 노드나 터미널의 집합이다. 이러한 연결은 대체로 유선 네트웍보다 적은 대역폭을 갖고, 각 노드가 라우터나 호스트로서의 역할을 한다. 이 네트웍 토폴로지는 노드간의 연결상태가 시간에 따라 변하므로 다이나믹하다[2]. 각 노드나 터미널은 PDA와 같은 이동성있는 소형 기기에 가깝다. 이 환경은 유선 네트웍과는 달리 key distribution center나 trusted third party같은 것이 존재하지 않는다. 만일 이들이 존재한다면 그 자체가 집중적인 공격대상이 되기쉽고, 각 노드들의 이동성이나 자율성에 제약요소로 작용할 것이므로 이 환경에서는 적합하지 않다.

2) Authentication

Authentication은 시스템의 사용 및 네트웍 자원의 사용을 요청하는 주체의 신원을 확인하는 것으로, 네트웍 보안의 기본적인 문제로 다루어져 왔다. 유선 네트웍에서는 public key를 이용한 Kerberos와 같은 authentication scheme들이 개발되어 왔다[5].

PKI를 이용한 authentication은 몇가지 문제를 가지고 있다. 첫째, 작은 기기들이 universal한 naming infrastructure에 의한 ID와 certificate를 가진다는 것은 그 용량에 비해 과중하여 비현실적이다. 둘째, 통신할 상대편을 찾았을때 그 상대편의 ID를 확인하는 절차가 매우 복잡하다. 셋째, 기기들의 peanut size의 CPU가 PKI 연산을 하기에 자원이 한정되어 있다는 것이다.

Dirk Balfanz et al[1]은 이 문제를 PKI 연산보다 경제적인 해쉬와 기존의 key exchange protocol(SSL, TLS, IKE 등)을 사용하여 PKI에 의존하지 않고 wireless network에서 authentication을 보장하는 방법을 제시했다.

2. 기존에 제시된 프로토콜

이 논문이 제시하는 프로토콜은 공간 제한적 채널에서의 pre-authentication과 wireless 채널에서의 authentication 두 부분으로 나누어진다. 먼저 물리적으로 제한된 환경에서 기기들이 서로의 public key 또는 그것을 대체할 수 있는 랜덤값의 해쉬를 교환한다. 이때 적외선 통신 등 단거리에 적합한 매개가 사용될 수 있다. 이 과정이 pre-authentication이며, 이 과정은 Anderson et al[6]의 작업에서 차용되었다. 이후 wireless 네트웍에서는 상호 교환한 정보를 사용, 기존의 key

exchange protocol을 통해 통신함으로써 authentication을 보장한다.

즉, 물리적으로 제한된 채널에서의 pre-authentication은,

A → B: $addr_A$, $h(PK_A)$
B → A: $addr_B$, $h(PK_B)$

또는 한쪽 상대방이 public key를 가지고 있지 않은 경우는

A → B: $addr_A$, $h(PK_A)$
B → A: $addr_B$, $h(S_B)$

등으로 응용할 수도 있다.

이후 wireless 네트웍에서 기존의 SSL/ TLS등을 이용한 authentication은,

A → B: TLS_CLIENT_HELLO

또는

A → B: PK_A
B → A: $E_{PK}(S_B)$

와 같이 이루어진다.

여기서 S_B는 B에 속한 secret 값, $h(S_B)$는 그 해쉬값, $E_{PK}(S_B)$은 A의 public key로 S_B를 암호화 한 값이다. $addr_A$, $addr_B$은 A(또는 B)가 갖는, wireless공간에서의 편의상의 주소이다.

그러나 PKI 없는 public key의 사용 보다는 프로토콜 전체를 해쉬 값만으로 구성하는 것이 올바른 PKI-독립적인 authentication protocol이다. 다음은 digital stream을 보내는데 주로 쓰이는 Guy Fawkes protocol의 단방향성을 개선한 interactive Guy Fawkes protocol이다.

물리적으로 제한된 채널에서의 pre-authentication은 보내고자 하는 메시지의 해쉬값과 그 authenticator의 해쉬값, 그 다음단계의 authenticator의 해쉬값을 보낸다.[1)]

Round 0:
A → B: $a_1=h(\underline{A_1}, h(X_2), X_1), h(X_1)$
B → A: $b_1=h(B_1, h(Y_2), Y_1), h(Y_1)$
A → B: $h(b_1, X_1)$
B → A: $h(a_1, Y_1)$

Wireless 채널에서는 이전 단계에서 해쉬한 값의 원본과 그 다음번 메시지의 해쉬값을 묶어서 보냄으로써 이전단계의 메시지의 무결성을 확인하고 다음 라운드를 bootstrap한다.

Round 1:
A → B: $\underline{A_1}=h(X_2), X_1, a_2= h(A_2, h(X_3), X_2)$
B → A: $B_1=h(Y_2), Y_1, b_2= h(\underline{B_2}, h(Y_3), Y_2)$
A → B: $h(b_2, X_2)$
B → A: $h(a_2, Y_2)$

Balfanz et al은 기존의 Guy Fawkes protocol을 양방향으로 하기위해서 A가 의미있는 메시지 $\underline{A_i}$를 보낸후, 의미있는 메시지 $\underline{B_i}$를 받기 전까지는 의미없는 메시지를 전달하도록 했다.

Round 2:
A → B: $A_2=h(X_3), X_2, a_3= h(A_3, h(X_4), X_3)$
B → A: $\underline{B_2}=h(Y_3), Y_2, b_3= h(B_3, h(Y_4), Y_3)$
A → B: $h(b_3, X_3)$
B → A: $h(a_3, Y_3)$

Round 3:
A → B: $A_3=h(X_4), X_3, a_4= h(\underline{A_4}, h(X_5), X_4)$
B → A: $B_3=h(Y_4), Y_3, b_4= h(B_4, h(Y_5), Y_4)$
A → B: $h(b_4, X_4)$
B → A: $h(a_4, Y_4)$

Round 4:
A → B: $\underline{A_4}=h(X_5), X_4, a_5= h(A_5, h(X_6), X_5)$
B → A: $B_4=h(Y_5), Y_4, b_5= h(\underline{B_5}, h(Y_6), Y_5)$
A → B: $h(b_5, X_5)$
B → A: $h(a_5, Y_5)$

A가 의미있는 메시지를 처음 보내고, 그다음 의미있는 메시지를 보낼 때 까지 이와 같은 주기가 반복된다.

3. 문제점

1) 처음의 authenticator가 이미 유출된 경우, authentication 보장이 안된다. 즉, authenticator나 해쉬된 메시지에 대해 passive attack을 받을 가능성이 있다.

3) Balfanz et al은 pre-authentication을 통해 상대방의 public key나 그 해쉬값 등의 정보를 교환한다는 가정하에 기존의 key exchange protocol을 사용, authentication을 보장하고 있다. 이는 사실상 이 절차가 상대방에 대한 사전지식을 공식적으로 갖게하는 절차에 지나지 않으며, 실제 물리적으로 제한된 공간에서의 근거리 pre-authentication은 기기들의 이동성을 제한한다.

II. 새롭게 제시하는 프로토콜

사용자간의 인증을 zero-knowldge proof기반의 프로토콜을 이용해, 물리적으로 제한된 공간에서의 pre-authentication절차 없이, 서로의 정보가 네트웍에 노출되지 않도록 하고, 기존의 interactive Guy Fawkes protocol을 이용하여 메시지의 무결성을 보장하는 프로토콜을 제안한다.

---

1) X_i, Y_i: authenticator로 사용되는 랜덤값
$h(Z_1, , Z_n)$: 연속된 $Z_1, , Z_n$ 의 단방향 해쉬값
A_i, B_i: 라운드 i 에서의 A(또는 B)로부터의 무의미한 랜덤 메시지
$\underline{A_i}$, $\underline{B_i}$: 라운드 i 에서의 A(또는 B)로부터의 의미있는 메시지
a_i, b_i: 라운드 i 에서의 A(또는 B)로부터의 commitment

1. zero-knowledge 기반의 프로토콜

Goldwasser et al에 의해 소개된 zero-knowledge proof는 상대방의 주장이 옳음을 증명하는 과정에서 상대방이 가진 어떤 정보도 유출하지 않는다. 이러한 특성으로 인해 cryptography분야에서 매우 각광받아왔다[4]. 본 논문에서는 ad-hoc wireless network에서 이 zero-knowledge proof를 사용자 인증시 사용할 것을 제안한다.

1) zero-knowledge authentication에 기반한 Fiat-Shamir protocol[3]

<가정들>

□ 공개적으로 알려진 RSA modulus n=pq가 있다.

□ 소수(素數) p 와 q 는 사용되거나 저장될 필요가 없다.

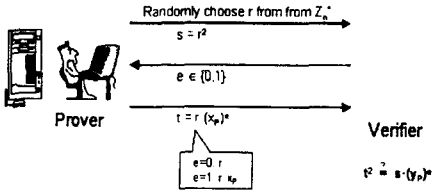
□ 모든 계산은 modulo n으로 수행된다.

□ 입증자 P'의 private key x_p 는 Z_n^*에서 임의로 선택된다.

□ 입증자 P의 public key는 y_p is the square of the private key y_p $(x_p)^2$ 인 쌍 (n, y_p)이다.

□ Z_n^*의 제곱근을 계산하는 것은 n을 인수분해하는것만큼 어렵다는 것이 수학적으로 입증되어 보여졌다.

□ 결론적으로, Fiat-Shamir protocol의 안전성은 인수분해의 어려움에 근거한다.



<그림1> Fiat-Shamir protocol round

이 프로토콜 라운드는 security parameter k만큼 반복된다.

2) 보안 분석

침입자가 각 라운드에서 올바른 e값을 예측할 가능성은 1/2이고 k 라운드에서는 $1/2^k$가 된다.

3) 적용된 프로토콜

위의 과정은 확률과 인수분해에 의한 상호인증을 수행한다.

기존의 SSL와 달리 상호인증 후, 보안성 있는 채널을 만드는 것이 아니라 상호인증으로만 끝나기 때문에 별도로 메시지 무결성을 보장하는 scheme이 필요하다. 이를 위해 interactive Guy Fawkes protocol을 이용하였다.

2. 특성

1) Pre-authentication 개념이 없다. 기존의 방식은 물리적으로 제한된 공간 안에서 상대방의 public key의 해쉬나 랜덤값의 해쉬를 교환하거나 또는 interactive Guy Fawkes protocol의 초기화 단계로서의 pre-authentication 과정을 거쳤다. 이것은 기기들의 이동성을 떨어뜨리며 실제 ad-hoc network에서의 효용성을 낮춘다.

2) Two-party 프로토콜만 전제한다. 기존의 interactive Guy Fawkes protocol이 그랬듯이 두 개의 기기만을 상정한다. 왜냐하면 multi-party에서 중앙에서 통제되는 네트웍이 형성된 경우, 일시적으로 형성된 group manager 역할을 하는 노드는 그룹키를 생성, 저장, 전파하므로 그 네트웍을 벗어나기 어렵고, 침입자의 표적이 되기 쉽기 때문이다. 그러나 통제되지 않는 네트웍에서는 브로드캐스트를 통해 그룹키를 공유할수 있을것이다.

III. 결론

기존에 제안된 논문이 다음번 메시지의 해쉬값을 미리 전달함으로써 다음 메시지를 bootstrap하는 방법으로 authentication을 한 반면, 새롭게 제시된 프로토콜은 기존의 authentication 과정에서 passive attack에 의해 authenticator가 노출될 경우를 배제하여 보다 강력한 authentication을 보장한다.

무엇보다 물리적으로 제한된 공간에서 pre-authentication을 하는 불편함을 없앴다. 이는 이동성을 높였다. 실제 ad-hoc network에서 사전에 상대에 대한 정보가 없는 상황에서의 이 이동성은 매우 유용할 것이다.

제안된 프로토콜은 전달하는 메시지의 무결성과 authentication을 보장하며, 사용자의 정보가 네트웍으로 유출되지 않으므로 eavesdropping이나 network sniffing등의 passive attack 에 대해서 안전하다.

그러나 메시지 교환부분은 여전히 passive attack에 노출되어있다. 따라서 이에 대한 대책이 연구되이야 한다.

IV. 향후과제

1) 메시지 교환시 가능한 passive attack에 대한 대책이 필요하다.

2) Ad-hoc wireless에서 zero-knowledge 프로

토콜을 사용한 실제적인 구현을 통해 실제 요구되는 자원의 양을 측정하는 것이 필요하다.

3) Group communication에 대한 방법 고안이 필요하다. Zero-knowldge 기반 프로토콜에서의 브로드캐스팅에 대한 구체적인 연구가 필요하다.

참고문헌

[1] D. Balfanz, D.K. Smetters, P. Stewart, and H. ChiWong, "Talking To Strangers: Authentication in Ad-Hoc Wireless Networks", in Proc. of the ISOC 2002 Network and Distributed Systems Security Symposium, February 2002.

[2] http://w3.antd.nist.gov/wctg/manet/

[3]http://www.ifi.unizh.ch/~oppliger/Presentations/AuthenticationProtocols/

[4]Zero-Knowledge: *a tutorial by* Oded Goldreich
http://www.wisdom.weizmann.ac.il/~oded/zk-tut02.html

[5] Sirbu, M.A. and J.C.-I. Chuang, "Distributed Authentication in Kerberos Using Public Key Cryptography", in Symposium on Network and Distributed System Security, 1997

[6] Frank Stajano and Ross Anderson. "The resurrecting duckling: Security issues for ad-hoc wireless networks". In Proceedings of the 7th International Workshop on Security Protocols, Lecture Notes in Computer Science. Springer-Verlag, Berlin Germany, April 1999.