Impersonation with the Echo Protocol

Yoo Chul Chung[0] Dongman Lee
Information and Communications University
{chungyc,dlee}@icu.ac.kr

에코프로토콜에서의 거짓 신원 공격

정유철[0] 이동만
한국정보통신대학교

1 Introduction

Knowing the physical location of an entity can be very useful. Such knowledge is useful for location-based access control or context-aware applications [2]. However, we must be able to ensure that we have the correct location of an entity for it to be a useful factor in access control.

Location determination is the problem of finding out where an entity is located at. In contrast, location verification verifies that an entity is indeed located at where it claims to be, where the entity somehow finds out the location by some other means. If the location determination mechanism is insecure, then we can use secure location verification to ensure that an entity is located at a certain location.

2 The Echo protocol

In Sastry et al. [3], which introduces the Echo protocol, the entity wishing to prove its location claim is called the *prover*, while the entity which wishes to verify the claim is called the *verifier*. The protocol verifies that the prover is located within a region centered around the verifier, which is called the verifier's *region of acceptance*.

The prover initiates verification by broadcasting its location. A verifier whose region of acceptance includes the location is selected. The verifier sends a nonce, which is a random bit string, to the prover by radio. After receiving the nonce, the prover sends it back to the verifier by ultrasound. If the nonce received by the prover is not the same as the one it sent, or if it took too long for the reply to be received, then the prover's location claim is rejected.

The Echo protocol itself does not require cryptography or time synchronization between provers and verifiers. It only needs a reasonably precise clock in the verifier and the means to communicate with radio and sound. It also does not require prearranged setup between verifiers and provers. This makes the protocol suitable for low-powered devices in spontaneous environments, e.g. ubiquitous computing or sensor networks [1].

3 Impersonation attack

The fact that the Echo protocol does not require prearranged setup nor cryptography is touted as an advantage. However, the protocol in its original form is unable to verify location claims in a useful way under these conditions. The problem is not that the protocol falsely verifies a location claim for a prover, but rather that anything else is unable to securely take advantage of the verification result.

An obvious way to use the Echo protocol for access control is to first verify the location of the prover, and then to grant access to the prover based on this verification result. Unfortunately, we cannot hide the identity of the prover without resorting to cryptography. If we wish to avoid the expense of cryptography, then we must assume

that the identity can be exposed to an adversary. The adversary can use this identity to obtain illegal access in a location-based access control system, using a form of run internal replay attack [4].

If we want to prevent an adversary from forging a message, the prover must use a secret known only to itself and perhaps the verifier. If the verifier does not possess the secret, then we require public key cryptography, or something at least as computationally expensive. Even if the verifier and the prover prearrange to share the secret, we will still require symmetric key cryptography or its equivalent

4 Defenses

The simplest way to prevent an impersonation attack is to just bear the cost of cryptography. Encrypting messages sent between the prover and the verifier after location verification finishes ensures that an adversary would not be able to send a valid forged message to the verifier.

By pre-sharing a secret key between the prover and the verifier, they can prevent adversaries from sending forged messages using symmetric cryptography. We could also avoid the need for prearrangements between the prover and verifier by using public key cryptography. We could actually use the *public key* of the prover as the identity. Using the Echo protocol, the verifier can confirm that the public key belongs to a prover that is located within its region of acceptance.

While using cryptography is a simple solution to preventing impersonation attacks, it is also an expensive one which negates one of the important advantages of the Echo protocol, which is its frugal use of resources. Fortunately, we can modify the Echo protocol so that it is resistant to impersonation attacks without having to use cryptography. The modification is very simple. Instead of sending the message after location verification, the prover sends the message when it first initiates location verification. We call the modified protocol the one-way variant of the Echo protocol.

The one-way Echo protocol is an inexpensive way to verify location claims, and is resistant to impersonation attacks. Like the original Echo protocol, the protocol itself does not require cryptography nor prearranged setup between provers and verifiers. Unlike the original protocol, messages such as access requests need not be encrypted, since message transmission is integrated into the protocol itself without opening the protocol to impersonation attacks.

5 Conclusions

Location verification, which verifies location claims made by provers, can be done using the Echo protocol. Unfortunately, we cannot securely take advantage of a verification result without using cryptography. This is because the Echo protocol has the following properties. First, it does not hide the identity of the prover. Second, an adversary can forge a message that can appear to be from the prover. Finally, a valid message can be received at any time by the verifier.

A simple way to defend against impersonation attacks is to lift the restriction against using cryptography. We suggest a one-way variant of the Echo protocol as an alternative. Although it is limited to sending short messages to the verifier when no reply is expected, it is resistant against impersonation attacks, while still maintaining the low resource requirements and spontaneity of the original Echo protocol.

References

[1] J. Hill, M. Horton, R. Kling, and L. Krishnamurthy. The platforms enabling wireless sensor networks. *Communications of the ACM*, 47(6):41–46, June 2004.

[2] E. Kaasinen. User needs for location-aware mobile services. *Personal and Ubiquitous Computing*, 7(1):70–79, May 2003.

[3] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *Proceedings of the 2003 ACM Workshop on Wireless Security*, pages 1–10. ACM Press, 2003.

[4] P. Syverson. A taxonomy of replay attacks. In *Proceedings of the 7th Computer Security Foundations Workshop*, pages 187–191. IEEE Computer Society Press, June 1994.