情報保護學會論文誌
第15卷 第5號, 2005. 10

인증 프로토콜과 Responsibility/Credit 개념에 관한 고찰*

박 동 국
순천대학교 정보통신공학부

Responsibility and Credit: New Members of the Authentication Family?*

DongGook Park
SunChon National University

ABSTRACT

There are several goals or properties which authentication protocols may have; some of them are key freshness, far-end aliveness, key confirmation, etc. Most of them have extensively been discussed and studied so far in the literature. "Responsibility" and "credit", which were first raised by Abadi as additional goals[1,2], received quite an exceptional treatment; there were little response from researchers about these new goals. It is surprising to see that these two properties have slipped through any investigation, successfully achieving the positions as the goals for authentication protocols. In this paper, we investigate these two new properties and their relations to authentication protocols, and answers to the question: what brings us credit and responsibility.

Keywords : *credit, responsibility, authentication protocols, key*

Ⅰ. Introduction

When it comes to the design and analysis of an authentication and key establishment protocol, the goals of the protocol is of paramount importance. Whether a claimed attack is possible or not is to be determined by whether the attack leads to a violation of the intended goals or not. While there is no perfectly agreed set of goals, most authors seems to agree that a few goals of the authentication protocols are essential, which are message freshness, far-end (or peer entity) aliveness, and key confirmation/authentication in the case that the authentication protocol is intended for key establishment as well.[4,7] Message freshness assures that authentication protocol messages are not replayed by attackers. Far-end aliveness means that a successful authentication protocol should convince the authenticating entity that the authenticated entity is out there right now for the current session. Key confirmation assures an entity that his peer entity is actually in possession of, or actually can calculate, the session key. Key authentication is the property whereby one party is assured

접수일 : 2005년 8월 16일 ; 채택일 : 2005년 8월 22일
* This research was supported by the MIC, Korea, under the ITRC support program supervised by the IITA.
주저자, dgpark6@sunchon.ac.kr

that no other party aside from a specifically identified (authenticated) second party may gain access to a particular secret key. Although there may be disagreement among authors on what these goals mean, they have been investigated and discussed in the literature.[4]

Abadi, who is well known for the BAN logic,[3] introduced two new notions, "responsibility" and "credit", which he calls "two facets of authentication".[1] Lecturers seem to introduce responsibility and credit as some basic properties of authentication protocols. An attack against a version of the EKE protocol in terms of credit was discussed in [5]. Formal analysis was applied to authentication protocols with regard to responsibility and credit.[6] In the main, however, these two newbies seem to have been accepted by researchers with little investigation about their very nature itself.

This paper describes what responsibility and credit mean, reviewing some example protocols as appeared in Abadi's original paper. We then discusses what brings us responsibility and credit, and investigate about the relation between identity and key, which seems to be a most interesting issue related to responsibility and credit.

II. Responsibility and Credit

Abadi noted that some protocols are adequate for assigning responsibility but not for giving credit, and vice versa. The following is from his own description about responsibility and credit.[1]

An "authenticated" message M from a principal A to a principal B may be used in at least two distinct ways:

- *B may believe that the message M is being supported by A's authority. For example, suppose that B is a file server, A a client, and M a request to delete a file f. Then B may use A's identity as an argument to the access control decision of whether to delete f.*
- *B may attribute credit for the message M to A. For example, suppose that B is running a contest, offering a prize to the principal that mails the factors for a large number. When B receives the message M as an entry, B may give credit for the entry to A.*

In this section, we describe responsibility and credit in detail using two example protocols, which are exactly the same protocols as those appeared in Abadi's paper.[1] In fact, Abadi used four example protocols, but we do not need all of them to understand responsibility and credit.

2.1 Responsibility

While the concept, "credit for a message M" is quite distinct from any other properties of authentication protocols, its dual concept (as Abadi claimed) "responsibility for a message M"is a bit confusing due to its apparent similarity to "non-repudiation". Let's have a look at a protocol which appeared in Abadi's paper.

Protocol 1. Encrypting a session key

1. $A \rightarrow B : \{A, K\}_{K_B}$
2. $A \leftarrow B : \{M\}_K$

Here, a principal A sends another principal B a session key K encrypted under B's public key K_B (message 1). Messages 2 is simply for illustration of the use of the session key K. Whenever A receives a message M encrypted under K as in message 2, A knows that it should be B that generated the message, or some principal

to which B gave K. So A can hold B responsible for M, because message 2 is clearly an indication of the possession of the secret session key K, which can be obtained only by B using B's secret private key. Here we can see that message 2 does not provide non-repudiation property. Therefore, Abadi's new notion "responsibility" is weaker than non-repudiation. In other words, when responsibility property is satisfied, then A knows it was B that sent the message M, but he cannot prove to a third party that it was B.

In the next example protocol, the borderline between non-repudiation and responsibility is rather blurred.

Protocol 2. Signing a public key

1. $A \rightarrow B$: $A, B, \{K, A, B, T\}_{K_A^{-1}}$
2. $A \rightarrow B$: $A, B, \{\{M\}_{K^{-1}}\}_{K_B}$

In the first message of Protocol 2, a principal A sends a short-term "public key" K to another principal B. The key, together with both principals' identity (A and B) and a timestamp T, is signed with A's long-term private key K_A^{-1} before transmission. The second message of the protocol shows an example of the use of K its corresponding private short-term key K^{-1} is used for signing a message M. Signed with A's long-term private key, message 1 can be interpreted as A's promise that he will be responsible for any message signed with the new short-term key K. This interpretation seems reasonable even when we consider the case that A is in fact not in possession of the corresponding short-term secret K^{-1} if A claimed a key then he must be in charge of the use of the key. Moreover, in Protocol 2 unlike Protocol 1, the short-term key is asymmetric key, and the message signed with its secret pair as in message 2 might be considered as a proof message to a third party.

In fact, by not requiring key confirmation (of K as in Protocol 2) as a necessary condition for "responsibility" property, Abadi provides a room for flexible application of the property: delegation of authority to another principal, say C. The key K may even be C's long-term public key; in such a case, the secret pair K^{-1} should never be disclosed to A. Through the protocol 2 with C's long-term public key as the value of K, A can entirely delegate his authority to C for a period of time. To make things fair, it should be said that this kind of quite dangerous delegation is never mentioned in Abadi's paper, where delegation is achieved only by A's delivering the short-term private key K^{-1} to C. This kind of delegation can be done with Protocol 1 as well: A simply delivers the symmetric session key K to C.

Although in his paper Abadi discusses about responsibility through more example protocols than the two protocols as described in this section, we believe that there is no missed point about responsibility.

2.2 Credit

Compared to its dual concept responsibility, credit is quite an unfamiliar notion, but its distinction from existing notions makes it easier to identify. The basic idea of credit as put forth by Abadi is that if a principal (not necessarily authenticated) X is the owner of a secret information M, the corresponding credit for M should go to the claimed identity, say A, by X. In other words, if it is undoubtedly obvious that the owner X of a secret message M claimed an identity A, then the credit for M goes naturally to A

(regardless of the authenticity of the claimed identity). Let's have a look again at Protocol 1, which is used in a different way than as in the previous section for responsibility. In the previous use of Protocol 1, the encrypted message M was delivered from B to A in the following example, however, a message M is sent from A to B.

Protocol 1. Encrypting a session key (with a different use)

1. $A \rightarrow B$: $\{A,K\}_{K_B}$
2. $A \rightarrow B$: $\{M\}_K$

Here again, the second message is shown for the use of the session key K. The meaning of message 1 is that a principal X who delivers a secret key K to B claimed an identity A. Note that A cannot choose K which has the same value as a key K' which has already registered with B by another principal, say C. For it means that A succeeded in attacking the encryption used in message 1 of Protocol 1. Also note that there is no verification (i.e. authentication) of the claimed identity A. Nevertheless, B can be assured that, upon receipt of a secret message M encrypted under K, its origin should be the owner of K, who is the originator of message 1. Now to whom should B give the credit for M? It should naturally be A because the owner of the secret message (hence the owner of K) claimed the identity A. The situation here is very similar to a real-life situation for banking. Someone X (not necessarily authenticated or even identified) may put money into a bank account of his own or someone else. (Of course, this kind of anonymous banking may not be allowed in some countries.)

As described in the previous section, Protocol 1 is also appropriate for holding B responsible for an encrypted message sent to A. What about Protocol 2, which was already shown adequate for responsibility purpose? We repeat the protocol below.

Protocol 2. Signing a public key

1. $A \rightarrow B$: $A,B,\{K,A,B,T\}_{K_A^{-1}}$
2. $A \rightarrow B$: $A,B,\{\{M\}_{K^{-1}}\}_{K_B}$

As stated before, the key K in this protocol is a short-term public key of a principal whose claimed identity is A. The first protocol message proves the recipient B that a principal who claims the identity A is actually A and he also claims that K is his own short-term public key. Is this proof enough for giving credit for a secret message M contained in message 2? Unfortunately, it is not because the following attack is possible as Abadi described.

An Attack against Protocol 2

1'. $C \rightarrow B$: $C,B,\{K,C,B,T\}_{K_C^{-1}}$
(intercepted by A)
1. $A \rightarrow B$: $A,B,\{K,A,B,T\}_{K_A^{-1}}$
2'. $C \rightarrow B$: $C,B,\{\{M\}_{K^{-1}}\}_{K_B}$
(intercepted by A)
2. $A \rightarrow B$: $A,B,\{\{M\}_{K^{-1}}\}_{K_B}$

In this attack, a principal A intercepts the first protocol message from another principal C to B, modifies it into message 1 and sends the result to B. Now the short-term public key K is registered with B as the key of the attacker A. When B receives a secret message M signed under the short-term private key K^{-1}, the credit for M is mistakenly given to the attacker A.

Abadi describes two ways to fix the protocol for credit purpose, both of which adds key confirmation to the original

protocol. We repeat them below with added fields enclosed in boxes.

Two ways to fix Protocol 2

1. $A \rightarrow B$: $A,B,\{K,A,B,T\}_{K_A^{-1}},\boxed{\{A\}_{K^{-1}}}$
2. $A \rightarrow B$: $A,B,\{\{M\}_{K^{-1}}\}_{K_B}$

or

1. $A \rightarrow B$: $A,B,\{K,A,B,T\}_{K_A^{-1}}$
2. $A \rightarrow B$: $A,B,\{\{\boxed{A},M\}_{K^{-1}}\}_{K_B}$

With key confirmation required to complete the fixed protocols, if A is an attacker to try to steal any other principal's short-term public key, A must sign his own name with K^{-1}, which is impossible because A is not the owner of K^{-1}.

Ⅲ. What Brings Us Responsibility and Credit?

Abadi noted that responsibility sometimes comes with signatures, while credit sometimes comes with encryptions. He noted also that a principal may take responsibility for the statements of another principal, or may defer credit for his own statements to another principal. Through these observations, he noted some duality between responsibility and credit. He states:

> *... A crisper understanding of this duality might lead to more regular protocol designs and to more systematic arguments about their correctness.*

Abadi, however, fails to lead us further beyond his description of two notions using example protocols. His investigation about credit and responsibility is unfortunately confined to specific example protocols; he failed to take his investigation up to the exposition of the concepts of two notions themselves. We believe, however, that Abadi's insight about responsibility and credit suggests a different angle to the relation between identity and key, which will be made clear in the next section. A formalization tried for credit and establishment, however seems to look the other way from the angle.[6]

As noted before, its apparent similarity to non-repudiation may be an obstacle to a crisper understanding of responsibility. Non-repudiation of a message M sent from A to B proves any third party that M could be generated only by A. Responsibility does not provide such a confidence to any entity except for the recipient B.

Responsibility. *Responsibility of a principal A to a principal B for a message M is justified if and only if B can be assured that A other than any principal said M.*

Hence non-repudiation is obviously a sufficient condition for responsibility. It should be noted that responsibility does not necessarily requires a message M be a secret message M may or may not be a secret message. A public message M signed by a principal A with his long-term private key provides non-repudiation and hence responsibility as well. A public message encrypted by a shared key K_{AB} between A and B also provides responsibility. If a message M is sent from A to B as a plaintext message, however, responsibility is supported only when it was a secret message to any principals but A and B up until it is said by A. Hence, responsibility captures the notion of message origin, not the notion of message secrecy. Consequently, the truth or falsehood of a message itself does not affect responsibility.

In fact, there seems to be not so much interesting point in responsibility itself. It becomes interesting when it is put together with credit, and more interesting when

these two properties are viewed with regard to identity and key, as described in the next section.

Credit is quite interesting because, unlike responsibility, credit for a message is not related to authentication of its origin. Credit may be confused with authority notion. Authority, however, should rather be related to responsibility as Abadi described. If somebody knows the answer to a contest quiz, he should be given due credit (such as a prize) regardless of which identity he claimed. Therefore, credit for a message M inevitably requires M to be a secret message. Furthermore, the credit giver, say B should be certain that M is not a fake information. That's enough for credit; B does not have to (and preferably in some cases should not) be concerned about whether the applicant (i.e., the credit receiver) is really A or not. Hence we note that credit can be obtained without authentication, and therefore anonymity and credit can be obtained together. This valuable point has been largely overlooked or even strongly objected.[6] The following description captures all these observations.

Credit0. *Credit for a secret message M to a credit applicant X is justified if and only if M is not a fake information.*

Note here that there is no stipulation of any identity of the applicant. This may sound a bit surprising when we recall the attack against Protocol 2, which was fixed by including the identity of the applicant signed under a short-term private key. If an applicant X presented M in person with a proof that he did not steal M from any other person, then there is never a need to identify who he is. If the message M, however, is delivered over a communication channel, then there should be a container, which the credit is to be put in. That is the only raison d'être of the identity data in a protocol for credit establishment protocol.

Authenticity of the credit giver, unlike that of the applicant, is essential to guarantee that the secret message M is not a fake one. For, with this not guaranteed, the applicant could have achieved M from a victim applicant by impersonating the credit giver to the victim. Confidential channel for a transmission of M is basically required to stop any interception. Therefore, we have the following conclusion.

Credit1. *A security protocol establishes due credit of an applicant X for a secret message M if and only if*

(i) the protocol provides a secure and authentic channel for M to the credit giver B, and

(ii) the protocol guarantees that the applicant claimed an identity, say A (regardless of its authenticity).

The most critical requirement for credit is the guarantee that an applicant is truly in possession of the relevant secret information. Provided that the applicant can prove his knowledge of the secret information without disclosing it, then the necessary and sufficient condition for credit come down to a much simpler version as follows.

Credit2. *Suppose a credit establishment protocol does not reveal a secret message M. Then, the protocol establishes due credit of an applicant X for M if and only if the protocol proves that X is in possession of M, and X claimed an identity.*

Note that the protocol satisfying the above condition is nowhere related to authentication of both the applicant and the credit giver. In other words, contrary to

Abadi's conjecture, *credit is not an aspect of authentication*. Recall that authentication of the credit giver is required only for the guarantee that the relevant secret message is not a fake one. Thus, with no need to disclose the secret message to prove possession, there is no need of authentication of either principals. Let's have a look at the following protocol.

Protocol 3. An "authentication free" credit only protocol

1. $A \rightarrow B$: $A, h(A, M)$

Here the applicant A hashes his own identity together with a secret message, e.g., an answer to a contest quiz issued by B, and sends the result to B. Assuming that B also knows the answer, B can check the hash value and verifies whether the originating principal knows the answer and the he has claimed the same identity as appeared in the plaintext field. The credit now goes to the principal A offline. If online delivery is preferred, the following modification may be added to Protocol 3.

A modification of Protocol 3

1. $A \rightarrow B$: $A, K, \{A\}_{K^{-1}}$
2. $A \rightarrow B$: $A, h(A, K, M)$
3. $A \leftarrow B$: $\{credit\}_K$

Here K is A's uncertified public key. Now, B is able to deliver a credit (for example, an e-book file) to A online as shown in message 3. Of course, without the assumption of B's a priori knowledge of the secret message M, Protocol 3 cannot be used for credit. In that case, we may consider the following protocol.

Protocol 4. "Authentication free" credit establishment protocol

1. $A \rightarrow B$: $A, K, \{A\}_{K^{-1}}$
2. $A \rightarrow B$: $A, \{\{M\}_{K^{-1}}\}_{K_B}$

Here again, message 2 appears as an example of the use of the K. Message 1 carries a proof that some principal X in possession of a secret information (i.e., K^{-1}) corresponding to K is claiming the identity A. Therefore, by **Credit2**, any credit for the secret information K^{-1} correctly goes to the claimed identity A. Message 1, as the only protocol message is not related to any authentication of the participating principals. Hence the protocol may be considered as "authentication free". However, if we consider message 2 as a part of the protocol, then it cannot be said to be authentication free. For the message reveals the included message only when a recipient party is really the authentic principal B. In this regard, Protocol 4 might be more closely related not to **Credit2** but to **Credit1**.

Ⅳ. Identity and Key

In the last section, we investigated responsibility and credit with respect to a principal and his message M. When we regard a short-term public key K or short-term private key K^{-1} as the message M, we can see an interesting duality between responsibility and credit, and their relation to entity authentication. To make their relation more noticeable, we concentrate only on "asymmetric" keys and also will use the following notation.

(X, K): A principal X (not authenticated yet) has claimed K as his own public key.

(A, K): An authenticated principal A has claimed K as his own public key.

(X, K^{-1}): A principal X (not authenticated yet) has claimed K as his own public key, and actually in possession of K^{-1}.

(A, K^{-1}): An authenticated principal A has

claimed K as his own public key, and actually in possession of K^{-1}.

We shall use this notation to capture the current status of an entity, say B's validated belief or information about his peer entity A and his asymmetric key.

Cryptographic entity authentication should be based on the assumption that an entity A is truly the owner of his asymmetric key pair K_A and K_A^{-1}. Upon this assumption, the statement "someone X is truly A" can be legitimately translated to a cryptographic statement "X has K_A^{-1} ". Authentication protocols are simply a procedure to validate the cryptographic statement. Therefore, when B runs a protocol to authenticate A, it is crucial that (entity, key)-status in B with regard to A should finally arrive at the belief (A, K_A^{-1}) after the protocol run.

Responsibility and credit can also be analyzed along a similar line of reasoning if we limit ourselves to a consideration of only the keys K and K^{-1} instead of the public or secret message M as appeared in the previous sections. The responsibility and credit as described Section 3 can be described using the notation introduced above, as follows.

Responsibility. *Responsibility of a principal A to a principal B for a short-term public key K is justified if and only if B can be assured of* (A,K).

Credit2. *A protocol establishes due credit of an applicant X for a short-term public key K if and only if B can validate the belief* (X, K^{-1}) *and X claimed an identity.*

Now, it becomes clear that responsibility and credit have a *duality* in the sense that responsibility requires the validation of the claimed identity, whereas credit requires the validation of the claimed public key K.

Consequently, if a protocol satisfies both responsibility and credit, it means that both the claimed identity and the public key K are correctly validated. In other words, the validated belief of B should be (A, K^{-1}). This, in turn, means that a principal A has been correctly authenticated (that is, his peer B validated the belief (A, K_A^{-1})), and also that A is the true owner of the short-term private key K^{-1} which he claimed using the relative public key K. Hence, we have the following conclusion.

Responsibility and Credit. *Successful authentication of a principal A and the key confirmation for a short-term private key* K^{-1} *of A is assured if and only if both responsibility and credit of A are correctly established for the use of* K^{-1} *at the same time(namely, the belief* (A, K^{-1}) are correctly validated*).*

Now we may interpret the essential premise (A,K_A^{-1}) for entity authentication to be a state where both responsibility and credit of the entity A for his long-term public key K_A are validated. In this respect, responsibility and credit can be said to be a dual facets of authentication. When it comes to a *short-term* public key K, however, credit establishment bears no relation to the authentication of the entity who claimed K. As described in the previous section, credit may not require authentication of the credit giver either if some assumption is justified.

V. Conclusion

We reviewed Abadi's novel notions, responsibility and credit, trying to capture an interesting features of them. Responsibility and credit of a principal A should

inevitably be related to a certain message or information M. The information M may or may not be a secret message for responsibility, whereas it should be a secret message for credit. Responsibility of a principal A for a message M inevitably requires authentication of A, and giving credit for M to a principal X is justified only when X proves his possession of M. If we consider a short-term private key K^{-1} as a special case of M, then credit is related to a sort of "authentication-free" key confirmation: that is, a confirmation that a principal X, whose identity is not authenticated, is in possession of K^{-1}. In fact, this kind of key confirmation is not sufficient for the establishment of credit: a stronger confidence is required, which may be called a sort of "entity authentication-free" or "pure" key authentication.[8] For an unauthenticated principal X may claim a short-term public key Kas his own key, which actually belongs to another unauthenticated principal Y. Entity authentication-free key authentication addresses exactly this concern. If we accept this terminology, then we may describe that responsibility and credit are justified by entity authentication and (pure) key authentication, respectively. As for credit establishment with responsibility not required, the required security protocol may be dramatically simplified as is the case with Protocol 3, its modified version, and Protocol 4.

Responsibility and especially credit come in several flavours, as we explored in previous sections, depending on what kind of information we regard as M. It may be a correct answer in a competition, a short-term private key, or even a long-term private key. As to the long-term asymmetric key, responsibility and credit turn out to be an exact dual notions of entity authentication. For the case of a short-term asymmetric key, responsibility and credit still shows a duality between them, but credit bears no relation to entity authentication of the principal who claimed the short-term key. When it comes to a secret message other than a key, then duality seems to be hardly justified; and under some environment, credit does not require entity authentication of neither principals of the applicant and the credit giver.

Credit looks more productive because it insinuates a possibility of entirely anonymous world for its being relatively free from entity authentication as discussed in the description of Protocol 3 in Section 3. Of course, several points remain to be settled; for example, how to do with responsibility for such an anonymous world.

References

[1] M. Abadi, "Two facets of authentication", *Proceedings of 11th IEEE CSFW*, pp. 27 33, 1998.

[2] M. Abadi, "Security Protocols and their Properties", *Foundations of Secure Computation*, NATO Science Series, IOS Press, Volume for the 20th International Summer School on Foundations of Secure Computation, pp. 39-60, 2000.

[3] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication", *DEC Systems Research Center*, Report 39, revised February 22, 1990.

[4] C. Boyd, "Towards extensional goals in authentication protocols", *DIMACS Workshop on Cryptographic Protocol Design and Verification*, 1997.

[5] A. Durante, R. Focardi, and R. Gorrieri, "CVS at Work: A Report on New Failures upon Some Cryptographic Protocols", *Proceedings of MMA-ACNS'01*,

Springer LNCS 2502, May 2001.
[6] R. Gorrieri, F. Martinelli, and M. Petrocchi, "A Formalization of Credit and Responsibility", *Proceedings of SASYFT 2004*. Available from http://www.iit.cnr.it/staff/fabio.martinelli/
[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
[8] D. Park, *Cryptographic Protocols for Third Generation Mobile Communication Systems*, PhD thesis, Queensland University of Technology, 2000.

〈著者紹介〉

박 동 국 (DongGook Park) 종신회원
1986년 2월: 경북대학교 전자공학과 졸업
1989년 2월: 한국과학기술원 전기 및 전자공학과 석사
2001년 9월: 호주 QUT (Queensland Univ. of Technology) 박사
〈관심분야〉 인증 및 키설정 프로토콜 모델링 및 분석