On Authentication between Human and Computer

Watanabe, Takahiro
Faculty of Information Science and Electrical Engineering, Kyushu University

Nohara, Yasunobu
Faculty of Information Science and Electrical Engineering, Kyushu University

Baba, Kensuke
Faculty of Information Science and Electrical Engineering, Kyushu University

Inoue, Sozo
Faculty of Information Science and Electrical Engineering, Kyushu University

他

出版情報：Pervasive Computing and Communications Workshops, pp.636-639, 2006-03
バージョン：
権利関係：

On Authentication between Human and Computer*

Takahiro Watanabe Yasunobu Nohara Kensuke Baba† Sozo Inoue
Hiroto Yasuura

Abstract

Electronic authentication with a portable device such as a smart card has been receiving increasing attention. An explosion of papers argues security on such kind of authentication, however the human concerned in an authentication is often regarded as his/her portable device. This paper considers an identification of a server computer of a service provider by a human with a portable device as a part of the authentication and an attack by a client computer which relays the communication between the portable device and the server computer. As a defense against the attack, we introduce a system with a portable device which has an interface to show information to a human.

1 Introduction

Recent years, electronic authentication have been receiving increasing attention by the explosive spread of computer networks. In authentication between a portable device such as a smart card and a server computer, it seems that various cryptographic technologies realize a secure mutual authentication, that is, a server identification by the human and a human identification by the server computer. A portable device which has sufficient computation ability can put into practice such a secure authentication even on a untruthful network [1, 3]. However, what our society requires is secure authentication between a "human" and a server computer, and it is not realized straightforwardly from secure authentication between a "portable device" and a server computer. For example, we know that an ideal authentication between a smart card and a server computer can provide a secure authentication also for the human who stole the card.

Biometrics is, in a sense, a solution to fill the gap between a human and a portable device. This technology guarantees the correspondence between a portable device and its owner in a human identification by a server computer. Hopper and Blum [2], and Matsumoto and Imai [4] argue human identifications by a computer, however a secure identification of a computer by a human tends to be regarded as one by a portable device. This paper takes a different approach to constructing a secure protocol on this kind of authentication, that is, we analyze a server identification by a human. Then, we consider security against a spoofing attack by a client computer which relays the communication between the human and the server computer. This argument is important since some technologies for secure authentication are constructed under the assumption that the client computer is trusted. For example, it is easily conceivable that, without confirming an ATM, an attack of spoofing as the ATM will success even for an ideal smart card with cryptographic and biometrics technologies.

In this paper, we consider a model of authentication between a human and a server computer with a portable device and a client computer, especially an identification of the server computer by the human. This model divides the human and the portable device explicitly, which makes clear the essence of the problem of an untruthful client computer. As a solution of this problem, we introduce an authentication system and an identification protocols with a portable device which has an interface to show information to a human.

2 Modeling Authentication Systems

The target of this paper is an identification of a server computer by a human. It is often confused with one by a portable device, hence we consider the following model of authentication systems which divides a human and a portable device explicitly.

The authentication model is constructed by the following four objects:

- a *server*, denoted by s, is a server computer of a service provider and wishes to verify a human as authentication;
- a *user*, denoted by u, is a human who wishes to have a service from a service provider and has a portable device;

*An edited version of this report was published in: *Proc. Fourth IEEE International Conference on Pervasive Computing and Communications (PerCom 2006) WORKSHOPS, pp.636–639, IEEE Computer Society, Mar, 2006.*

†Faculty of Information Science and Electrical Engineering, Kyushu University, *baba@i.kyushu-u.ac.jp*

- a *token*, denoted by t, is a portable device which has a computation ability for a secure mutual authentication with other computers;
- a *client*, denoted by c, is a computer which relays the communication between a service computer and a portable device and has an interface to give information to a human.

Then, we assume that a token and a server can operate a secure mutual authentication, that is, they send information for the authentication each other and the information gives no knowledge to the other objects. Moreover, a client can know any information sent between a token and a server, however the token or the server can know whether the client tampered the information.

Now we formalize the communications between objects as follows:

- a server can send information to a client;
- a token can send information to a client;
- a client can send information to a server, a user, and a token.

Under the previous situations, (a trial of) a mutual authentication between a user and a server is operated as follows:

1. the server and the token of the user operate a mutual authentication;
2. the token sends the result $r_{tc} \in \{1, 0\}$ of the authentication to the client;
3. the client sends the result $r_{cu} = r_{tc}$ to the user,

where 1 and 0 correspond to information that the server was accepted/rejected by the token. The procedure is illustrated in Fig. 1.

By the assumption, a mutual authentication between the token and the server is operated securely at the first step. If the server can confirm the correspondence between the token and its owner (for example, by a technology of biometrics), the server can identify the user. On the other hand, as to the identification of the server by the user, the user can not confirm whether $r_{tc} = r_{cu}$. Therefore, the client can success the attack to connect with a fake server computer besides tampering the information.

In this paper, we consider an identification of a server by a user with a trusted token and an attack by a client against the identification. A protocol of an identification of a server by a user is *valid* if the user can know that the server is rejected (even if the user can not know that the server is accepted). It is clear that no protocol can be valid on the previous model since the client can send $r_{cu} = 1$ for $r_{tc} = 0$ if the client is an attacker.

3 Authentication System for Valid Protocol

We introduce a model of an authentication system which realizes a valid protocol of the identification of a server computer by a human. This model is essentially an extension with respect to the communications of the objects.

The problem on the model in the previous section is that the user can know the result of the authentication between the token and the server only by the information from the client. A straightforward solution is to consider a protocol of authentication of the client by the user which guarantees the correctness of the information from the client. This solution is realized, for example, by a password (as a challenge of authentication of the client) of user. Another solution is to establish a connection from a trusted object to the user for the result of the authentication. In this section, we consider a model which has a connection from the token to the user, that is, we add to the communication in the previous section the following condition:

- a token can send information to a user.

On the model of the previous connection, a mutual authentication between a user and a server is operated as follows:

1. the server and the token of the user operate a mutual authentication;
2. the token sends the result $r_{tu} \in \{1, 0\}$ of the authentication to the user.

This situation is illustrated in Fig. 2.

By the assumption that the token is trusted, r_{tu} is equal to the result of the authentication. Therefore, the protocol of the server identification is valid.

4 Conclusion

We introduced a model of authentication between a human and a server computer with a trusted token and a client computer. In the model, we argued about an identification of the server computer by the human and an attack by the client computer. As a conclusion, the attack can be prevented if the user can know whether $r_{cu} = r_{tc}$, and this condition is satisfied by a token which has a interface to the human.

References

[1] Fiat, A. and Shamir, A.: "How to prove yourself: Practical solutions to identification and signature

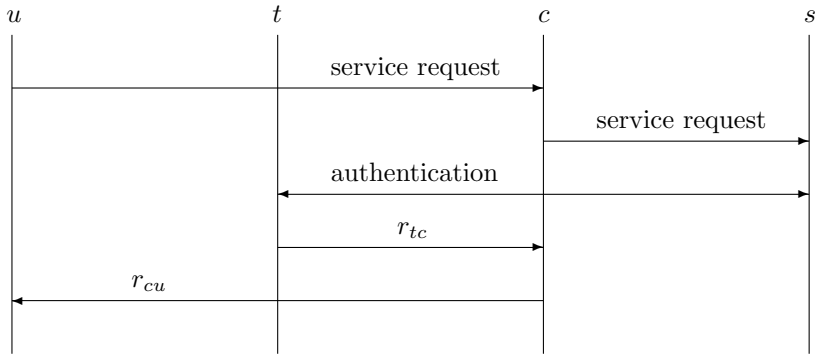

Figure 1: A procedure of authentication of a server computer by a user.

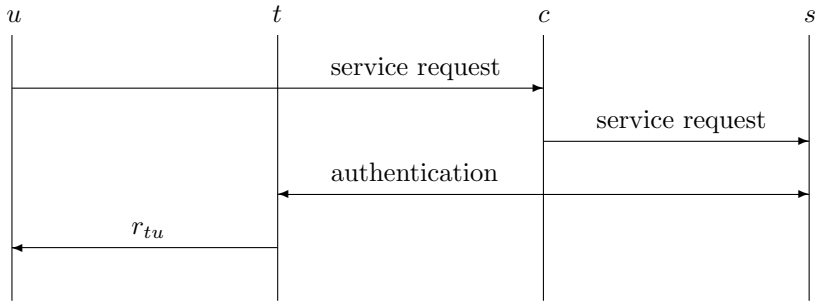

Figure 2: A procedure of authentication of a server computer by a user with a token which has a interface to the user.

problems", Lecture Notes in Computer Science, vol.263, pp.186–194, 1987.

[2] Hopper, N.J. and Blum, M.: "Secure Human Identification Protocols", Lecture Notes in Computer Science, vol.2248, pp.52–66, 2001.

[3] Lamport, L.: "Password Authentication with Insecure Communication", Communications of the ACM, vol.24, no.11, pp.770–772, 1981.

[4] Matsumoto, T. and Imai, H.: "Human Identification Through Insecure Channel", Lecture Notes in Computer Science, vol.574, pp.409–421, 1991.