Impersonation Problems in Remote Authentication Using Biometrics

Vladimir.B. Kropotov
Department of Information Security Bauman Moscow State Technical University kropotov@ieee.org

Abstract. A number of recently proposed authentication protocols have serious restrictions. This paper characterizes the criteria and gives formal definitions about possible *Server* impersonations as *User* or another *Server* for highlighted protocols. This paper demonstrates that published protocols unable to reach mutual authentication if shared information derived from the same biometric feature for more than one server. Hence if user doesn't store or publicize any information situation where server and user share some kind of secret is not equal to mutual authentication. Paper introduces formal definition of *Recoverable Information (RI).RI* allows new authentication protocol construction. In this protocol user mustn't publicize any information and is able to authenticate servers even if authentication information derived from the same biometric feature for more than one server.

1 Preliminaries

This paper uses adopted terminology from [DRS04] and [BDK+05]. Let U is a user, who enrolled into biometrics based authentication process. User personal biometric secret ω and secret value $Priv_U$ which is shared between user U and server *Srv* isn't equal. Pub_U is a public value which derived from user personal secret ω. Let S is a set of servers: $(Pub_U, Priv_U) \leftarrow S$ i.e. servers from S hold some public and private information about user U.

2 Recently Proposed Methods and Impersonation Problems

2.1 Improved Solution Tailored for Mutual Authentication and Impersonation Problems

Reconstruction of protocol from paragraph 4.1 in [BDK+05]. Let Π be a PAK protocol and let (SS,Rec) be a well-formed secure sketch. Construct a modified protocol Π' as follows:

Initialization. User U samples ω_0 according to W_0 (i.e., takes a scan of his biometric data) and computes $Pub_U \leftarrow SS(\omega_0)$. The user registers (ω_0, Pub_U) at the server *Srv*.

Protocol execution (server). The server sends Pub_U to the user. Then it executes protocol Π using the following parameters: it sets its own "identity" (within Π) to be $Srv \,||\, Pub_U$, its "partner identity" to be $Pid = U \,||\, Pub_U$, and the "password" to be ω_0.

Protocol execution (user). The i^{th} time the user executes the protocol, the user first samples ω_i according to distribution W_i (i.e., the user re-scans his biometric data). The user also obtains a value Pub'_U in the initial message it receives, and computes $\omega' = Rec(\omega_i, Pub'_U)$. If $\omega' = \perp$ then the user simply aborts. Otherwise, the user executes protocol Π, setting its own "identity" to $U \,||\, Pub'_U$, its "partner identity" to $Srv \,||\, Pub'_U$, and using the "password" ω'.

Definition 1. Let SU is a set of substances: $\forall su \in SU; \exists i: (\omega_{f,i}, Pub_{su}) \leftarrow su; |SU| > 1 \Leftrightarrow$ *any substance able to impersonate itself as user*. In other words, if user U shares the same biometric feature f between more than one substance when any substance able to impersonate itself as user.

Proposition 1. Let $\omega_{f,i}$ is the i^{th} scan of biometric feature f for user U. If $\exists S' \subseteq S : (\omega_{f,i}, Pub_{i,U}) \leftarrow S'$, where f is fixed value, $i \in Z^+ \bigcup \{0\}$ and $|S'| > 1 \Leftrightarrow$ *any server able to impersonate itself as user*.

2.2 The Application of a Robust Fuzzy Extractor to Achieve Mutual Authentication or Authenticated Key Exchange Over an Insecure Channel and Impersonation Problems

Reconstruction of protocol from paragraph 3.3 in [BDK+05]:

Given any secure protocol Π (say, for authenticated key exchange) based on a uniformly distributed shared key of length l, any $(m,l,n,\varepsilon,t,\delta)$ -robust fuzzy extractor (Ext,Rec), and any source W_0 with $H_\infty(W_0) \geq m$, consider the protocol Π' constructed as follows:

Initialization. The user U samples ω_0 according to W_0 (i.e., takes a scan of his biometric data) and computes $(Priv_U, Pub_U) \leftarrow Ext(\omega_0)$. The user registers $(Priv_U, Pub_U)$ at the server *Srv*.

Protocol execution. The i^{th} time the user wants to run the protocol, the user first will sample ω_i according to distribution W_i (i.e., the user re-scans his biometric data). The server sends Pub_U to the user, who then computes $Priv'_U = Ext(\omega_i, Pub_U)$. If $Priv'_U = \perp$ then the user immediately aborts. Otherwise, the server and user execute protocol Π, with the server and the user respectively using the keys $Priv_U$ and $Priv'_U$.

Definition 2. Let SU is a set of substances, $(Priv_{su}, Pub_{su}) \leftarrow Ext(\omega_{f,i})$, $Pub_{su}=(x,s)$, $s \leftarrow SS(\omega_{f,i})$, and x is a random. If $(\forall su \in SU; \exists i: (Priv_{su}, Pub_{su}) \leftarrow su; |SU| > 1) \Leftrightarrow$ *any substance able to impersonate itself as another substance*. In other words, we have more than one substance with interchangeable pairs $(Priv_{su}, Pub_{su})$ then any substance able to impersonate itself as another substance from SU.

Proposition 2. Let $\omega_{f,i}$ is the i^{th} scan of biometric feature f for user U, $Pub_U=(x,s)$, $s \leftarrow SS(\omega_{f,i})$, x is random, $(Priv_{i,U}, Pub_{i,U}) \leftarrow Ext(\omega_{f,i})$. If $\exists S' \subseteq S: (Priv_{i,U}, Pub_{i,U}) \leftarrow S'$, where f is fixed, $i \in Z^+ \bigcup \{0\}$ and $|S'| > 1 \Leftrightarrow$ *any server from* S' *able to impersonate itself as another*.
According to *Proposition 2* if more than one servers share pairs $(Priv_{i,U}, Pub_{i,U})$ which based on the same biometric feature *f* of user *U*, then user able only to identify server and mutual authentication is not possible. This situation occurs because user unable to store even public value and must trust everyone who have a valid pairs $(Priv_{i,U}, Pub_{i,U})$.

2.3 "Zero Storage" Remote Biometric Authentication and Impersonation Problems

Detailed protocol descriptions shown in [Boyen04].

Proposition 3. Let $\omega_{f,i}$ is the i^{th} scan of biometric feature f for user U, $Pub_U=(x,s)$, $s \leftarrow SS(\omega_{f,i})$, x is random, $(Priv_{i,U}, Pub_{i,U}) \leftarrow Ext(\omega_{f,i})$. If $\exists S' \subseteq S: (Pk_{Priv_{i,U}}, Pub_{i,U}) \leftarrow S$, where f is fixed value, $Pk_{Priv_{i,U}}$ signed public key for user *U*, $i \in Z^+ \bigcup \{0\}$ and $|S'| > 1 \Leftrightarrow$ any server from S' able to impersonate itself as another.
Proposition 3 means that user unable to authenticate server.

2.4 Enhanced protocol for mutual authentication

Definition 3. *Recoverable Information (RI)* - information which user must not store, but must to know at the time the authentication with specified server is taking place. This information must be unique for every server, where user is enrolled.

Example 1. If user wants to participate in authentication session with server iu8.bmstu.ru, he must know at least server name immediately before authentication.

Proposition 4. Let $\omega_{f,i}$ is the i^{th} scan of biometric feature f for user $U, Pub_{U,Srv}=(x,RI_{Srv},y,s)$, and $y = HASH(\omega_{f,k}, x, RI_{Srv})$. If we substitute $Pub_U=(x,s)$ to $Pub_{U,Srv}=(x,RI_{Srv},y,s)$ and user U trusts only himself, then the *mutual authentication* is possible.
In this case *U* signs his public value with biometrics based personal key. Information RI_{Srv} ensures that there's the only one server *Srv* from *SU* (as defined in Definition 2) able to store $Priv_{U,Srv}$ associated with $Pub_{U,Srv}$.

Protocol

We use protocol from paragraph 2.2 as a basis. Given any secure protocol Π (say, for authenticated key exchange) based on a uniformly distributed shared key of length l, any $(m,l,n,\varepsilon,t,\delta)$ -robust fuzzy extractor (Ext,Rec), and any source W_0 with $H_\infty(W_0) \geq m$, consider the protocol Π' constructed as follows:

Initialization. The user U samples ω_0 according to W_0 (i.e., takes a scan of his biometric data) and computes $(Priv_{U,Srv}, Pub_{U,Srv}) \leftarrow Ext(\omega_0)$ as in *Proposition 4*. The user registers $(Priv_{U,Srv}, Pub_{U,Srv})$ at the server *Srv*.

Protocol execution. The i^{th} time the user wants to run the protocol, the user first will sample ω_i according to distribution W_i (i.e., the user re-scans his biometric data). The server sends $Pub_{U,Srv}$ to the user, who then computes $Priv'_{U,srv} = Ext(\omega_i, Pub_{U,Srv})$. If $Priv'_{U,Srv} = \perp$ then the user immediately aborts. User recovers ω_0 using ω_i and $Pub_{U,Srv}$, next checks his signature in $Pub_{U,Srv}$ and ensures server identity. If signature not valid then the user immediately aborts. Otherwise, the server and user execute protocol Π, with the server and the user respectively using the keys $Priv_{U,Srv}$ and $Priv'_{U,Srv}$.

References

[DRS04] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Proc. Advances in Cryptology—Eurocrypt '04, 2004.

[BDK+05] Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Secure remote authentication using biometric data. In Ronald Cramer, editor, Advances in Cryptology—EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science, pages 147–163. Springer-Verlag, 2005.

[Boyen04] Xavier Boyen. Reusable cryptographic fuzzy extractors. In Eleventh ACM Conference on Computer and Communication Security. ACM, October 25–29 2004.