# Biometric Identity Trust: Toward Secure Biometric Enrollment in Web Environments

Florian Obergrusberger, Baris Baloglu, Johannes Sänger, and Christian Senk

University of Regensburg
Department of Management Information Systems
93053 Regensburg, Germany

**Abstract.** The nonrepudiation of a biometric authentication depends on the authenticity of the corresponding biometric profile. If the enrollment process is not controlled by some trusted entity, a user's biometric data might be misleadingly linked to another person's digital identity. To secure the biometric enrollment in open Web-based environments, we propose the biometric observer principle: An arbitrary trustworthy person observes an individual's enrollment at a biometric identity provider and confirms this to the system. The concept rests on a specified trust model, which assesses the trustworthiness of both the observer and the authenticity of an observed biometric profile. Trust relations between observer and observed persons are managed by the authentication system. We implemented a cloud-based biometric identity provider to validate and demonstrate the proposed concept.

**Keywords:** Authentication, Biometrics, Identity Management, Trust.

## 1 Introduction

Effective access control to cloud resources requires a high quality of user authentication [18]. A possible way to achieve strong authentication in a very flexible way is the employment of cloud-based biometric authentication services [20]. Before a biometric authentication is possible, an enrollment process has to be passed in order to register a biometric template with the biometric system [9,15]. Therefore it might be necessary to secure the enrollment by restricting access to legitimate persons only. Additionally, this persons have to accomplish the process correctly. To achieve such a secure enrollment, we propose the biometric oberver principle which applies basic ideas from the Web of Trust concept.

The remainder of this paper is structured as follows: Section 2 defines biometrics and secure biometric enrollment. Section 3 refers to the relevant basics of trust and trust models. In Section 4, the conceptual basics for the convergence of trust models with a secure enrollment and a prototype implementation are provided. Section 5 discusses the presented approach and Section 6 summarizes the results and directs future research.

M. Yousif, L. Schubert (Eds.): Cloudcomp 2012, LNICST 112, pp. 124–133, 2013.

## 2 Securing the Biometric Enrollment

Biometric authentication is defined as the automated identification or verification of a person using behavioral or physiological characteristics such as fingerprint, palmprint or keystroke dynamics [15]. Basic requisition for an effective biometric authentication is (besides the security and performance of the biometric authentication) a secure prior enrollment [8,9]. Enrollment describes the process where an individual's biometric feature is registered in form of a digital template with the biometric system [15]. After the enrollment is successfully completed the biometric system can be run in two different modes, verification or identification, to authenticate an enrolled user [9]. In verification mode, a user provides his claimed identity and a biometric sample, which is then checked against the corresponding biometric profile stored at the system (1:1 comparison). When operating in identification mode, a user only provides a biometric sample and the biometric system determines the corresponding digital identity based on all available templates (1:n comparison). Compared to traditional authentication techniques based on knowledge (passwords) or tokens, biometric features are inherently and naturally bound to a person. This implicates potential increases regarding both the practicability and nonrepudiation of an authentication [15]. Especially in cases where a person's digital identity is involved in legally binding transactions, a proofable binding between digital identity and the corresponding natural person reduces the risk of fraudulent behavior such as identity theft. To ensure the authenticity of a biometric profile, a trusted entity verifies a natural person's identity by specified means (e.g. identification document) and supervises this person's enrollment process afterward. The observer confirms the enrollment's correct (and secure) accomplishment by authenticating to the biometric system with his own biometric sample.

## 3 Trust and Trust Models

At first, this section introduces the notion and characteristics of trust. Then some trust models, especially the Web of Trust, are introduced.

### 3.1 Defining Trust

The notion of trust is a topic that has been discussed in research for years. Although trust has already been analyzed in detail in various disciplines there is no generally accepted definition [13]. This is on the one hand due to the fact that trust is often associated with terms like credibility, reliability or confidence [21]. On the other hand, trust can be contemplated in a cognitive, emotional and behavioral dimension [21]. Oxford Dictionary defines trust as "firm belief in the reliability, truth, or ability of someone or something" [19]. This definition is very close to the definition of "reliability trust", which can be found in literature regarding online trust and reputation systems (e.g. eBay) [17]. Moreover, trust has several characteristics. The following list shows some properties that are important in respect of this work [6,14]:

- *Subjectivity*: Trust is always perceived individually;
- *Fuzziness*: There is a smooth transition between trust and distrust;
- *Direction*: Trust is unidirectionally bound to an entity;
- *Conditional transitivity*: Trust can be transitive. With transitivity, the level of trust decreases.

In order to establish trust toward an entity, different trust models have emerged.

### 3.2 Trust Models

In literature, various types of trust models can be found. An accepted classification differentiates between policy-based trust and reputation-based trust [2,22]. Policy-based systems mostly address the problem of authorization and access-control [2]. To establish trust, credentials are exchanged [22]. An example for the usage of credentials is the login on a computer, where username and password have to be provided. The possession of these credentials proof the administrator's trust toward the user [2]. In a reputation-based model in contrast, trustworthiness is measured by means of collective referrals or ratings [2,17]. Oxford Dictionary defines reputation as “the beliefs or opinions that are generally held about someone or something” [19]. Hereby the subjective trust is deduced from a combination of personal experience and referrals obtained over social networks or across trust paths [2,22]. For trust paths, transitivity is an important characteristic. Two parties don't need to have direct information about each other, they can rely on the information of a trusted third [2]. A trust model that takes advantage of this property is the Web of Trust. The following example is commonly used to describe this coherence.

Alice, a friend of Carol's knows that Bob's public-key certificate is authentic. Therefore she signs it. Carol however doesn't know Bob. If they want to communicate in private, Bob hands over his public-key certificate. Carol doesn't know if it is authentic by herself. But she sees that Alice signed and trusts it. Hence Carol can trust Bob's certificate in a transitive way [1].

## 4 Concept and Implementation

Subject of this section is the design and implementation of a system which ensures the authenticity of a biometric profile in open environments. Authenticity refers to the profile's genuineness and trustworthiness by means of a definite identity [10]. For this purpose, we introduce the role of the *observer*, which is a trusted person that supervises the enrollment process.

### 4.1 Biometric Observer or Four-Eyes Principle

The authenticity of the biometric data captured during the enrollment process should be verified by a trusted instance to prevent fraudulent use. Especially when the enrollment is conducted at home or at an open registry point, this is difficult to implement. For that reason we developed the biometric observer or four-eyes principle, which shall enable a flexible and efficient protection. With this principle, an arbitrary user which is already enrolled, the so-called observer, vouches for the authenticity of the enrollment process and can guarantee for the originality of the biometric profile. The validation of the user identity can be tied to different guidelines. A schematic flow is shown in Figure 1.

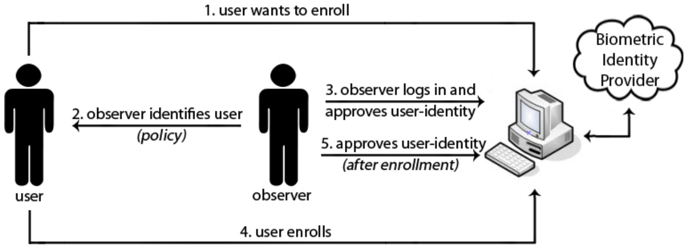
1. user wants to enroll
Biometric Identity Provider
3. observer logs in and approves user-identity
2. observer identifies user
(policy)
5. approves user-identity
(after enrollment)
user
observer
4. user enrolls

**Fig. 1.** Schematic Flow (Observation)

1. A user wants to create a biometric profile. Therefore he starts the enrollment process, where the name and, if necessary, various identity-related attributes are handed over.
2. To ensure the authenticity of the profile, an already enrolled user, the observer, acts as trusted instance and checks the identity of the user.
3. The observer logs in with his biometric profile, verifies the identity of the enrolling user and, if required, specifies by which means this verification was conducted.
4. The user starts providing his biometric data (enrollment).
5. When the enrollment process is completed, the observer approves the accuracy of the process.

By means of this method, trust can be established across several steps. If Alice observed Bob for example, she can trust Carol's and Dave's profiles transitively, whose enrollment processes were observed by Bob. The level of trust however decreases in this coherence. These trust relations can be described within a directed graph. Every profile is represented through a node in the graph and the relations are directed edges. In this scenario, the distance of two nodes is crucial for the level of reliability.

In a model where Alice observes Bob during the enrollment process (Figure 2), Bob in contrast just is observed and does not prove the identity of his observer (Alice), there is only a one-way relationship. Hereby every single user builds his own tree of trust with himself being the anchor. As a consequence, Alice will never be part of Bob's tree of trust, since there are only trust relations to one's followers. From a global perspective this leads to a hierarchy, a tree with the system administrator on top of it as global trust anchor that enrolled at the beginning without observation. To establish a Web of Trust, in which all nodes can potentially trust each other, a subsequent approval of a profile's

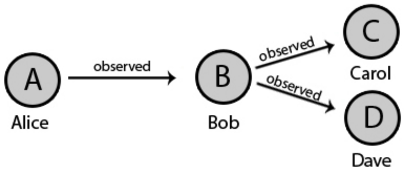

**Fig. 2.** Trust Relationship Tree

authenticity must be possible, to build a bilateral trust relationship. This takes us to the second method to proof the authenticity of a profile, the *confirmation.*

In contrast to the observation process, the confirmation is carried out between two already enrolled users. Analogous to the observer, the role of the confirmer is introduced. Figure 3 shows a generic confirmation process. With the confirmation, bilateral trust relations can be established. Moreover, the trustworthiness can be increased after the completion of the enrollment process. This leads to a Web of Trust.

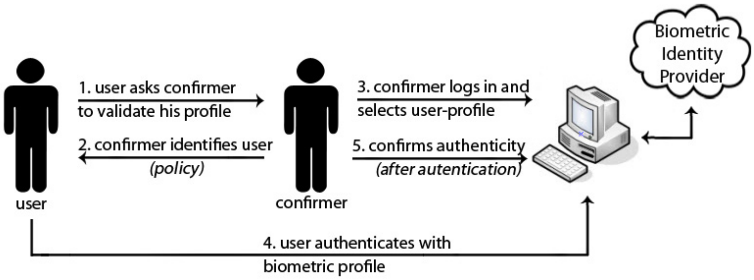
Biometric Identity Provider
1. user asks confirmer to validate his profile
2. confirmer identifies user (policy)
3. confirmer logs in and selects user-profile
5. confirms authenticity (after autentication)
user
confirmer
4. user authenticates with biometric profile

**Fig. 3.** Schematic Flow (Confirmation)

In Figure 4 Alice observed Bob's enrollment and Bob confirmed the authenticity of Alice's biometric profile afterward. Hence there is a bilateral trust relationship. The relation between Alice and Dave however is different. Alice can trust Dave's profile transitively. Dave confirmed the validity of Alice's profile and therefore has a direct trust relation toward Alice.

### 4.2 Trust Metric

To make the level of trust measurable, a trust metric is necessary. Since the literature concerning trust metrics has been growing rapidly during the last years, a lot of trust metrics exist [11]. Some of them could certainly be used to solve this problem. In this work we point out what requirements a trust metric has to meet and what it could look like. The described metric should be understood as an example. As mentioned in section 3.1, trust is subjective

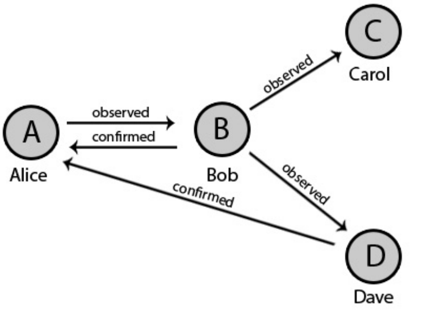

**Fig. 4.** Bilateral Trust Relationship (Web)

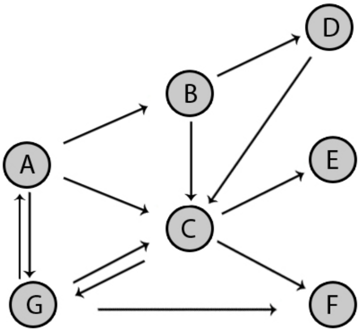

**Fig. 5.** Web of Trust (Global View)

and perceived individually. Thus the metric has to represent the level of trust customized from the perspective of each node. Hereby the distance of two nodes, by reason of the decreasing level of trust with transitivity, and the reputation of a node in the Web of Trust have to be included. The problem in general is to some extend related to the rating problem regarding websites in the Google search algorithm. The so-called PageRank calculates the reputation level of a website on base of the reputation of the linking pages [7]. In contrast to the PageRank, the trust level of a node in this metric is no global value. It has to be calculated individually from the perspective of each node. Hence, the following requirements were set up for the metric:

1. The node, from whose perspective the trust value of the other nodes is measured, is the "root" node. All edges to the root node are not considered. The root node has the trust value 1.
2. A trust value is calculated for all nodes of the web that can be reached over a trust path from the root node. The trust values of these nodes are within the interval $]1;\infty[$. The closer the trust value is to 1, the higher is the level of trust. For all nodes that can't be reached from the root over a trust path, the value 0 is assigned. The value 0 means that there is no trust relationship at all. Additionally the maximal length of a trust path can be defined in order to limit the size of the web.
3. The final trust value is calculated on base of two factors: (a) the direct trust factor, which is the distance between the root and a considered node. The distance is the length of the shortest path between two nodes. The length is the number of edges a path uses. The distance between any node and itself is 0. With every additional node on the trust path the distance is increased by 1. (b) the reputation factor, which includes the reputation derived from all trust paths that point to the node. A node must not appear twice in a trust path.

These requirements lead us to the following exemplary recursive function, inspired by the PageRank:

$$T_A(N_X) = \underbrace{d(N_A, N_X)}_{direct-trust-factor} + \underbrace{\left(e^{r\left((\sum_{i=1}^{n} \frac{-1}{T_A(N_i))}\right)}\right)}_{reputation-factor}$$

$T_A(N_X)$: *Trust Value of a node X from node A's perspective*
$d(N_A, N_X)$: *Distance between node A and node X*
$r$: *Reputation weight parameter*

*To calculate the trust value of a node X, $T_A(N_X)$, the length of the shortest path to node X is determined. Then the reputations factor corrects the value depending on its reputation. The parameter r can be chosen individual in order to weight the importance of the reputation factor. In our example r=0.75.*

To demonstrate this function, an example is provided. Figure 5 shows an exemplary Web of Trust. The paths show directed trust relations, derived from observation or confirmation. In Figure 6 it is evident that the trust value increases (the trust level decreases), while moving away from the root node A. Node C has the highest level, apart from the root, because it is very near to A and has a high reputation in the web. Node B however has a considerably lower level, because there are no other trust paths but the one from Node A (Figure 7). Node F has a comparatively high trust level since there are trust paths from high level nodes (C and G) although it has no direct relation to the root. From node B's perspective, the trust values are different. Node A for example has a significant low level compared to the other nodes, because the transitive trust path has a length of 4.

Since observation and confirmation are rated equally in this metric, the obervation could be renounced during the enrollment process. In this case, a profile is untrusted at the beginning. The scope of an untrusted profile however must be restricted until the authenticity is proved by confirmation. This supports scenarios where a minimum level of enrollment security (and quality) is required.

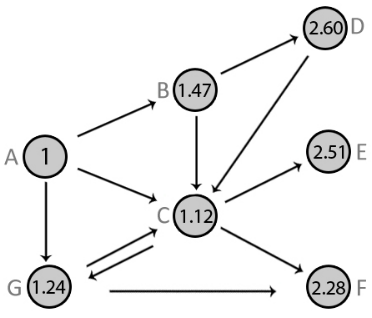

**Fig. 6.** Trust Values (Perspective A)

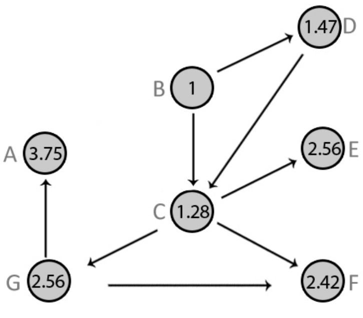

**Fig. 7.** Trust Values (Perspective B)

### 4.3 Prototype Implementation

To implement the described observer principle, a cloud-based biometric authentication system was developed. Biometric systems require suitable biometric reading devices (sensors) to collect and to digitize an individual's biometric raw data [15]. Here, it explicitly depends on the respective applied method, which kind of sensor is needed. For instance, whereas voice, face, or keystroke data can be acquired with common and standardized devices such as microphones, webcams and computer keyboards, procedures like iris or fingerprint recognition require specific dedicated sensors, thus restricting the applicability of such methods. Consequently, for the application in open environments (e.g. public cloud computing), the former methods are preferable. Below, we particularly apply keystroke dynamics. Keystroke dynamics is determined by unique characteristics such as speed, rhythm and the continuity and precision of typing [4,5]. These characteristics are represented by a combination of key events, that is, pressing and releasing of a key as well as hold and transition periods [3,16].

The current prototype implementation of the four-eyes principle allows the biometric system's administrator to enable an observed enrollment for new users. In this case the administrator is in charge of selecting observers to supervise new users' enrollment processes. The biometric system's administrative graphical user interface allows the assignment of a certain observer and invites the respective user to enroll. This invitation is sent via e-mail which also contains a one-time access token to the enrollment application. This collects typing samples from the user and generates the biometric template. After the user successfully finished the enrollment process the application demands for the observer to authenticate biometrically. Thus it is possible for new users to create a biometric profile and enroll all over the world, as long as an observer is available.

## 5 Discussion

This work aims for increasing the security of the biometric enrollment process by implementing the four-eyes principle. Here, the quality and security of the biometric authentication system is out of scope and not considered by the model developed. For a secured enrollment, an observer already known to the biometric system supervises the enrollment process of another person. The observer verifies this physical person's identity and then confirms the binding to the digital identity created. Therefore the observer's trust in observed persons' digital identities is strengthened.

Referring to the Web of Trust model, other individuals trusting the observer's digital identity also benefit from the observed enrollment. Because the newly enrolled user's digital identity is on their trust path, the conditional transitivity of trust allows them to calculate a trust value for it. Another positive effect of such an observed enrollment is the possibility to decrease the number of failed enrollments. Since the observer has to be enrolled to the biometric system, he is already familiar with the enrollment process and can help the enrolling person to avoid mistakes. The proposed four-eyes principle can be used for both operational modes of biometric systems, verification and identification, since both modes aim for authenticating a person and confirm the binding between digital identity and the natural person behind. Because biometric profiles and trust relations are maintained by the biometric system, it is responsible to ensure the authenticity of this data. If a person wants to prove his trust in other persons' digital identities, he cannot do this on his own, he has to rely on the information provided by the biometric system instead. A decentralized approach in which participants inform each other about their trust relations would release the biometric system from maintaining the trust relations, but ensuring the authenticity of the biometric profiles would still lie in the biometric system's area of responsibility.

Because a user to be observed and a potential observer do not initially know each other, the user has to discover a qualified one and physically meet him. This requires efforts regarding coordination and travelling and is not explicitly supported by the system proposed.

## 6 Conclusion

To secure the biometric enrollment in Web-based environments, we propose the biometric observer principle and provide a respective prototype implementation. The concept applies major ideas of the Web of Trust. The supervision of a user's enrollment by an observer increases the authenticity of the created biometric template. A comprehensive trust model enables the subjective formalization of the trustworthiness of the biometric identities of both observers and other entities. The relations between observer and observed persons are maintained in the system's database.

Future work should include the design of a user-based trust-metric configuration and the convergence of the four-eyes principle with a public key infrastructure to allow users to sign trust paths and biometric templates.

## References

1. Abdul-Rahman, A.: The PGP Trust Model. EDI-Forum: The Journal of Electronic Commerce 10(3), 27–31 (1997)
2. Artz, D., Gil, Y.: A survey of trust in computer science and the semantic web. Web Semant. 5(2), 58–71 (2007)
3. Bakdi, I.: Benutzerauthentifizierung anhand des Tippverhaltens bei Verwendung fester Eingabetexte. Universitäts Verlag, Regensburg (2007)
4. Bartmann, D., Bakdi, I., Achatz, M.: On the Design of an Authentication System Based on Keystroke Dynamics Using a Predefined Input Text. International Journal of Information Security and Privacy 1(2), 1–12 (2007)
5. Bergando, F., Gunetti, D., Picardi, C.: User Authentication through Keystroke Dynamics. ACM TISSEC 5(4), 367–397 (2002)
6. Bless, R., Mink, S., Blaß, E.-O., Conrad, M., Hof, H.-J., Kutzner, K., Schöller, M.: Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen. Springer, Berlin (2005)

7. Brin, S., Page, L.: The anatomy of a large-scale hypertextual web search engine. Comput. Netw. ISDN Syst. 30(1-7), 107–117 (1998)
8. Dorfner, M.: Evaluation und Weiterentwicklung von Zertifizierungsverfahren für biometrische Systeme: Eine exemplarische Betrachtung von Zertifizierungsverfahren mit dem Schwerpunkt IT-Sicherheit. Schriftenreihe Studien zur Wirtschaftsinformatik, Kovač (2012)
9. Dotzler, F.: Datenschutzrechtliche Aspekte und der Einsatz biometrischer Systeme in Unternehmen: Eine exemplarische Betrachtung von Systemen auf der Grundlage des biometrischen Merkmals Tippverhalten. Kölner Wissenschaftsverlag, Köln (2010)
10. Eckert, C.: IT-Sicherheit: Konzepte, Verfahren, Protokolle, 6th edn. Oldenbourg, München (2009)
11. Gómez Mármol, F., Martínez Pérez, G.: State of the art in trust and reputation models in P2P networks. In: Handbook of Peer-to-Peer Networking, pp. 761–784. Springer (2010)
12. Grandison, T., Sloman, M.: A survey of trust in internet applications. IEEE Communications Surveys Tutorials 3(4), 2–16 (2000)
13. Herzig, A., Lorini, E., Huebner, J.F., Vercouter, L.: A logic of trust and reputation. Logic Journal of IGPL 18(1), 214–244 (2010)
14. Huang, J., Fox, M.S.: An ontology of trust: formal semantics and transitivity. In: Proceedings of the 8th International Conference on Electronic Commerce: The New e-commerce: Innovations for Conquering Current Barriers, Obstacles and Limitations to Conducting Successful Business on the Internet, ICEC 2006, pp. 259–270. ACM, New York (2006)
15. Jain, A., Flynn, P., Ross, A. (eds.): Handbook of Biometrics. Springer, New York (2007)
16. Janakiraman, R., Sim, T.: Keystroke Dynamics in a General Setting. In: Lee, S.-W., Li, S.Z. (eds.) ICB 2007. LNCS, vol. 4642, pp. 584–593. Springer, Heidelberg (2007)
17. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decis. Support Syst. 43(2), 618–644 (2007)
18. Mather, T., Kumaraswamy, S., Latif, S.: Cloud security and privacy (an enterprise perspective on risks and compliance), 1st edn. Theory in practice. O'Reilly, Sebastopol (2009)
19. Oxford Dictionaries (visited on April 15, 2012)
20. Senk, C., Dotzler, F.: Biometric Authentication as a Service for Enterprise Identity Management Deployment: A Data Protection Perspective. In: Sixth International Conference on Availability, Reliability and Security, ARES 2011, Vienna, Austria, pp. 43–50. IEEE (2011)
21. Wang, Y.D., Emurian, H.H.: An overview of online trust: Concepts, elements, and implications. Computers in Human Behavior 21, 105–125 (2005)
22. Work, F., Bonatti, P.A., Shahmehri, N., Duma, C., Olmedilla, D., Nejdl, W., Baldoni, M., Baroglio, C., Martelli, A., Coraggio, P., Antoniou, G., Peer, J., Fuchs, N.E.: Rule-based policy specification: State of the art and future work (2004)