1. Introduction

This In banking applications, user authentication is traditionally based on username and password, come forth biometric solutions allow biometric data during session establishment. But in Unimodal biometric approach still a single verification is considered and the identity of the user is permanent during the entire session. A secure protocol is defined for constant authentication through continuous user verification. Biometric techniques offer solution for secure and trusted authentication. The user’s identity has been verified, the system resources are available for fixed period of time and identity of the user is constant during whole session. The proposed system detects misuses of computer resources and prevents malicious activities based on multi-modal biometric continuous authentication. Biometric and user data's are stored in smart phones. Security of web-based application is very important as there is increase in complexity of cyber attacks. Biometric application provides more security for authentication process than proving the username and password. Bio-metric user authentication is typically formulated as a “single shot” providing user verification only during login phase when one or more biometric traits may be required. Once the user’s identity has been verified, the system resources are available for a fixed period of time or until explicit logout from the user. This approach assumes that a single verification is sufficient, and that the identity of the user is constant during the whole session. For example: consider a user is already logged into the critical service and then and leaves the PC in the work area as a while. This problem is even risky when it is used in mobile phones in public and crowded areas as the device can be lost while the session is active. The users are authenticated and it can be misused easily. To detect the misuses of the computer resources and prevent that from the unauthorized user replaces an authorized one by providing the solution based on the multimodal biometric continuous authentication turning the user authentication as the continuous process rather than the one time occurrence. To avoid that a single biometric trait is forged, biometrics authentication can rely on multiple biometrics traits. Finally, the use of biometric authentication allows credentials to be acquired transparently, i.e. without explicitly notifying the user or requiring his/her interaction, which is essential to guarantee better service usability. Face can be acquired by using the front camera but not purposely for the acquisition of the biometric data for example the user may be reading a textual SMS or watching a movie on the mobile phone. Key-stroke data can be acquired whenever the user types on the keyboard, for example when writing an SMS, chatting, or browsing on the Internet.

This paper presents a new approach for user verification and session management that is applied in the CASHMA (Context Aware Security by Hierarchical Multilevel Architectures) system for secure biometric authentication on the Internet. CASHMA is able to operate securely with any kind of web service, including services with high security demands as online banking services, and it is intended to be used from different client devices e.g., smart phones and Desktop PCs. CASHMA is used for highly secure, a user session is a continuous sequential multi-modal biometric authentication protocol which computes and refreshes session time outs based on the client. In the CASHMA context, each subsystem comprises of all the hardware/software elements necessary to acquire and verify the authenticity of one biometric trait, including sensors, comparison algorithms and all the facilities for data transmission and management.

2. Proposed System

Continuous Authentication (CA) systems represent a new generation of security mechanisms that continuously monitor user behavior and use this as basis to re-authenticate periodically throughout a login session. A problem in continuous authentication is that it aims to tackle the user device. (smart phone, laptop, etc.) when it is used, stolen or
forcibly taken after the user has already logged into the services. The proposed approach assumes that first the user logs in using a strong authentication procedure, and then a continuous verification process is started based on multi-modal biometric. Similarly, when a multi-modal biometric verification system is presented, it continuously verifies the presence of a user working with a computer. If the verification fails, the system reacts by locking the computer and by delaying or freezing the user’s processes.

In CASHMA assessment, the choice of ADVISE was mainly due to: i) its ability to model detailed adversary profiles, ii) the possibility to combine it with other stochastic formalisms as the Mobius multi-formalism, and iii) the ability to define ad-hoc metrics for the system we were targeting.

### 3. The Cashma Framework

The CASHMA authentication service includes: i) an authentication server, which interacts with the clients, ii) a set of high-performing computational servers that perform comparisons of biometric data for verification of the enrolled users, and iii) databases of templates that contain the biometric templates of the enrolled users. Users have to be registered to the CASHMA authentication service, expressing also their trust threshold.

#### 2.1 Representation of the Protocol:

The continuous authentication protocol allows providing adaptive session timeouts to a web service to set up and maintain a secure session with a client.

A. Basic Definitions:

Given n unimodal biometric sub-systems Sk, with k = 1, 2, …, n that are able to decide independently on the authenticity of a user, the False Non-Match Rate, FMRk, is the proportion of genuine comparisons that result in false non-matches. False non-match is the decision of non-match when comparing biometric samples that are from same biometric source (i.e., genuine comparison). It is the probability that the unimodal system Sk wrongly rejects a legitimate user. Conversely, the False Match Rate, FMRk, is the probability that the unimodal subsystem Sk makes a false match error i.e., it wrongly decides that a non-authorized user is instead a legitimate one (assuming a fault-free and attack-free operation). Obviously, a false match error in a unimodal system would lead to authenticate a non-legitimate user. To simplify the discussion but without losing the general applicability of the approach, hereafter we consider that each sensor allows acquiring only one biometric trait; e.g., having n sensors means that at most n biometric traits are used in the sequential multimodal biometric system.

The user trust level gu(t) indicates the trust placed by the CASHMA authentication service in the user u at time t, the global trust level trust(u, t) describes the belief that at time t the user u in the system is actually a legitimate user, considering the combination of all subsystems trust levels mt(Sk=1,…,n, t) and of the user trust level gu(t). The trust threshold gmin is a lower threshold on the global trust level required by a specific web service; if the resulting global trust level at time t is smaller than gmin (i.e., g(u,t) < gmin), the user u is not allowed to access to the service. Otherwise if g(u,t) ≥ gmin the user u is authenticated and is granted access to the service.

The execution of the protocol is composed of two consecutive phases: the initial phase and the maintenance phase. The initial phase aims to authenticate the user into the system and establish the session with the web service. During the maintenance phase, the session timeout is adaptively updated when user identity verification is performed using fresh raw data provided by the client to the CASHMA authentication server.

The user (the client) contacts the web service for a service request; the web service replies that a valid certificate from the CASHMA authentication service is required for authentication.
2.1.1 Initial phase:

Using the CASHMA application, the client contacts the CASHMA authentication server. The first step consists in acquiring and sending at time $t_0$ the data for the different biometric traits, specifically selected to perform a strong authentication procedure (step 1). The application explicitly indicates to the user the biometric traits to be provided and possible retries.

The CASHMA authentication server analyzes the biometric data received and performs an authentication procedure. Two different possibilities arise here. If the user identity is not verified (the global trust level is below the trust threshold $g_{min}$), new or additional biometric data are requested (back to step 1) until the minimum trust threshold $g_{min}$ is reached. Instead if the user identity is successfully verified, the CASHMA authentication server authenticates the user, computes an initial timeout of length $T_0$ for the user session, sets the expiration time at $T_0 + t_0$, creates the CASHMA certificate and sends it to the client (step 2).

The client forwards the CASHMA certificate to the web service (step 3) coupling it with its request. The web service reads the certificate and authorizes the client to use the requested service (step 4) until time $t_0 + T_0$.

2.1.2 Maintenance Phase:

When at time $t_i$ the client application acquires fresh (new) raw data (corresponding to one biometric trait), it communicates them to the CASHMA authentication server (step 5). The biometric data can be acquired transparently to the user; The CASHMA authentication server receives the biometric data from the client and verifies the identity of the user. If verification is not successful, the user is marked as not legitimate, and consequently the CASHMA authentication server does not operate. If verification is successful, the CASHMA authentication server applies the algorithm to adaptively compute a new timeout of length $T_i$, the expiration time of the session at time $t_i + T_i$, and then it creates and sends a new certificate to the client. The client receives the certificate and forwards it to the web service; the web service reads the certificate and sets the session timeout to expire at time $t_i + T_i$.

2.1.3 Identification:

Given an input biometric sample, identification determines if the input biometric sample is associated with any of a large number (e.g., millions) of enrolled identities. Typical identification applications include welfare disbursement, national ID cards, border control, voter ID cards, driver’s license, criminal investigation, corpse identification, parenthood determination, missing children identification, etc. These identification applications require a large sustainable throughput with as little human supervision as possible.

Conclusion

In existing system initial one time login verification is inadequate to address the risk involved in post logged in session. Therefore this project attempts to provide a continuous iris authentication system. Continuous multi-modal iris authentication verification with improves security and usability of user session.

Reference


