CONTINUOUS USER IDENTITY BASED VERIFICATION FOR SECURE INTERNET SERVICES

D.Soundharya[1], P.Pavithra[2], S.Dhivithana[3], S.Kowsalya[4], Dr. M.Ramesh Kumar[5]
[1,2,3,4] III year Students, Department of Computer Science and Engineering,
VSB College of Engineering Technical Campus, Coimbatore, Tamilnadu, India.
[5]Associate Professor, Department of Computer Science and Engineering,
VSB College of Engineering Technical Campus Coimbatore, Tamilnadu, India.

ABSTRACT

Session management in distributed Internet services is traditionally based on username and password, explicitlogouts and mechanisms of user session expiration using classic timeouts. Emerging biometric solutions allow substituting username and password with biometric data during session establishment, but in such an approach still a single Verification is deemed sufficient and the identity of a user is considered immutable during entire session. Additionally, the length of the session time out may impact on usability of the service and consequent client satisfaction. This paper explores promising alternatives offered by applying biometrics in the management of sessions .A secure protocol is defined for perpetual authentication through continuous user verification. The protocol is determines adaptive timeouts based on the quality, frequency and type of biometric data transparently acquired from the user.

Keywords: Internet services, biometric solutions, session time, authentication and data transparency.

1 INTRODUCTION

SECURE user authentication is fundamental in most of modern ICT systems. User authentication systems are traditionally based on pairs of username and password and verify the identity of the user only at login phase. No checks are performed during working sessions, which are terminated by an explicit logout or expire after an idle activity period of the user.

Security of web based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber attacks; biometric techniques offer emerging solution for secure and trustedauthentication, where username and password are replaced by biometric data. However, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially considering their possible application financial and banking sectors.

Such observations lead to arguing that a single authentication point and a single biometric data cannot guarantee a sufficient degree of security . In fact, similarly to traditional authentication processes which rely on username and password, biometric 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 (at the beginning of the session) is sufficient, and that the identity of the user is constant during the whole session. For instance, we consider thissimple scenario: a user has already logged into a security-critical service, and then the user leaves the PC unattended in the work area for a while.

To timely detect misuses of computer resources and prevent that an unauthorized user maliciously replaces an authorized one, solutions based on multimodal biometric continuous

authentication are proposed, turning user verification into a continuous process rather than a onetime occurrence. 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. We present some examples of transparent acquisition of biometric data. Face can be acquiredwhile the user is located in front of the camera, but not purposely for the acquisition of the biometric data; e.g., the user may be reading a textual SMS or watching a movie on the mobile phone. This approach differentiates from traditional authentication processes, whereusername/password are requested only once at login time or explicitly required at confirmationsteps; such traditional authentication approaches impair usability for enhanced security, and offer no solutions against forgery or stealing of passwords. 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., smartphones, Depending on the preferences and requirements of the owner of the web service, the CASHMA authentication service can complement a traditional authentication service, or can replace it.

The approach we introduced in CASHMA for usable and highly secure user sessions is a continuous sequential (a single biometric modality at once is presented to the system) multimodal biometric authentication protocol, which adaptively computes and refreshes session timeouts on the basis of the trust put in the client. Such global trust is evaluated as a numeric value, computed by continuously evaluating the trust both in the user and the (biometric) subsystems used for acquiring biometric data. In the
acquire and verify the authenticity of one biometric trait, including sensors, comparison algorithms and all the facilities for data transmission and management. Trust in the user is determined on the basis of frequency of updates of fresh biometric samples, while trust in each subsystem is computed on the basis of the quality and variety of sensors used for the acquisition of biometric samples, and on the risk of the subsystem to be intruded.

2.PRELIMINARIES

2.1 Continuous Authentication

A significant problem that continuous authentication aims to tackle is the possibility that the user device (smartphone, table, laptop, etc.) is used, stolen or forcibly taken after the user has already logged into a security critical service, or that the communication channels or the biometric sensors are hacked.

The work in proposes a multi-modal biometric continuous authentication solution for local access to high-security systems as ATMs, where the raw data acquired are weighted in the user verification process, based on i) type of the biometric traits and ii) time, since different sensors are able to provide raw data with different timings. Point ii) introduces the need of a temporal integration method.

2.2 Basic Definitions

The basic definitions that are adopted in this paper. Given n unimodal biometric sub systems Sk, with $k= 1, 2, \ldots, n$ that are able to decide independently on the authenticity of a user, the False Non-Match Rate, $FNMRk$, 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 legitimate 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 loosing 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 our sequential multimodal biometric system.

The user trust level $g(u, t)$ indicates the trust placed by the CASHMA authentication service

in the user *u* at time *t*, i.e., the probability that the user *u* is a legitimate userjust considering his behavior in terms of device utilization (e.g., time since last keystroke or other action) and the time since last acquisition of biometric data.

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 authenticatedand is granted access to the service.

3. EXISTING SYSTEM

Security of web-based applications is a serious concern, due to recent increase in frequency and complexity of cyber-attacks. The biometric techniques offer emerging solution for secure and trusted authentication, where username and password are replaced by biometric data. The users identity has been verified, the system resources are available for a fixed period of time or until explicit logout from the user so single verification is processed in the user authentication and identity of the user is constant during whole session.

3.1. Disadvantages

- Parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing especially financial and banking sectors application.
- The impostors can impersonate user and access strictly personal data. The services where users are authenticated can be easily misused.

4. PROPOSED SYSTEM

The proposed system detect misuses of computer resources and prevent an unauthorized user maliciously replaces an authorized one based on multi-modal bio-metric continuous authentication. The proposed system performs user verification process in a continuous manner rather than one time occurrences. The use of biometric authentication allows credentials to be acquired transparently without explicitly notifying user interaction that is essential to guarantee better service usability.

4.1. Advantages

- The proposed system presents new approach for user verification and session management that is applied in CASHMA(Context Aware Security by Hierarchical Multilevel Architectures) system for providing secure biometrics authentication on the internet.
- The CASHMA is able to operate securely with any kind of web service, including services with high security demands as online banking services.
- The proposed system is intended to use from different client devices e.g. smart phones, desktop pc and biometric kiosks at entrance of secure areas.
- Depending on the preferences and requirements of the owner of the web services, the CASHMA authentication services can complement a traditional authentication service , or can replace it.

5.CASHMA ARCHITECTURE

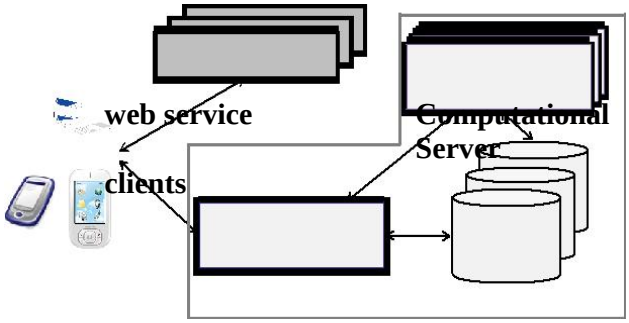
5.1 Overall View of the System

The overall system is composed of the CASHMA authentication service, the clients and the web services connected through communication channels. Each communication channel implements specific security measures which are not discussed here for brevity.

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 en-rolled users, and
iii) databases of templates that contain the biometric templates of the enrolled users (these are required for user authentication/verification).
The web services are the various services that use the CASHMA authentication service and demand the authentication of en-rolled users to the CASHMA authentication server. These services are potentially any kind of Internet service or application with requirements on user authenticity.
They have to be registered to the CASHMA authentication service, expressing also their trust threshold. If the web services adopt the continuous authentication protocol, during the

registration process they shall agree with the CASHMA registration office on values for parameters h, k and s .

Finally, by clients we mean the users' devices (laptop and desktop PCs, smartphones, tablet, etc.) that acquire the biometric data (the raw data) corresponding to the various biometric traits from the users, and transmit those data to the CASHMA authentication server as part of the authentication procedure towards the target web service. A client contains i) sensors to acquire the raw data, and ii) the CASHMA application which transmits the biometric data to the authentication server. The CASHMA authentication server exploits such data to apply user authentication and successive verification procedures that compare the raw data with the stored biometric templates. Privacy issues still exist due to the acquisition of data from the surrounding environment as for example voices of people nearby the CASHMA user, but are considered out of scope for this paper. The continuous authentication protocol explored in this paper is independent from the selected architectural choices and can work with no differences if templates and feature sets are used instead of transmitting raw data, or independently from the set of adopted counter measures.



CASHMA authentication service

5.2 Sample Application Scenario

The smartphone contacts the Online Banking service, which replies requesting the client to contact the CASHMA authentication server and get an authentication certificate. Using the CASHMA application, thesmartphone sends its unique identifier and biometric data to the authentication server for verification. The authentication server verifies the user identity, and grants the access if: i) it is enrolled in the CASHMA authentication service, ii) it has rights to access the Online Banking service and, iii) the acquired biometric data match those stored in the templates database associated to the provided identifier. In case of successful user verification, the CASHMA authentication server releases an authentication certificate to the client, proving its identity to third parties, and includes a timeout that sets the maximum duration of the user session. The client presents this certificate to the web service, which verifies it and grants access to the client.

The CASHMA application operates to continuously maintain the session open: it transparently acquires biometric data from the user, and sends them to the CASHMA authentication server to get a new certificate. Such certificate, which includes a new timeout, is forwarded to the web service to further extend the user session.

5.3 The CASHMA certificate

The information contained in the body of the CASHMA certificate transmitted to the client by the CASHMA authentication server, necessary to understand details of the protocol.

Timestamp and sequence number univocally identifyeach certificate, and protect from replay attacks.

6.THE CONTINUOUS AUTHENTICATION 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. The timeout is adapted on the basis of the trust that the CASHMA authentication system puts in the biometric subsystems and in the user. .

6.1 Description of the Protocol

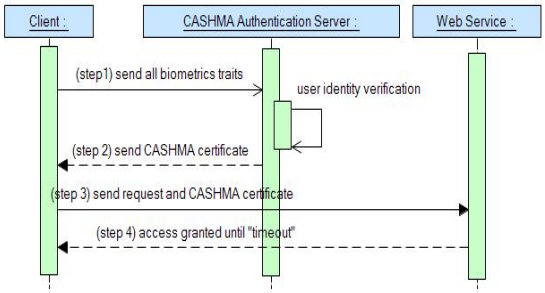
The proposed protocol requires a sequential multi-modal biometric system composed of *n* unimodal biometric sub-systems that are able to decide independently on the authenticity of a user.

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.

Initial phase. This phase is structured as follows

- 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



- Using the CASHMA application, the client contacts the CASHMA authentication server. The first step consists in acquiring and sending at time $t0$ the data for the different biometric traits, specifically selected to perform a strong authentication procedure . 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 *gmin*), new or additional biometric data are requested until the minimum trust threshold *gmin* is reached. Instead if the user identity is successfully verified, the CASHMA authentication server authenticates the user, computes an initial timeout of length $T0$ for the user session, set the expiration time at $T0 + t0$, creates the CASHMA certificate and sends it to the client.

- The client forwards the CASHMA certificate to the web service coupling it with its request.
- The web service reads the certificate and authorizes the client to use the requested service until time $t0 + T0$.

Maintenance phase.

It is composed of three steps:

- When at time *ti* the client application acquires fresh (new) raw data (corresponding to one biometric trait), it communicates them to the client may explicitly notify to the user that fresh biometric data are needed.

- 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 to refresh the session timeout. This does not imply that the user is cut-off from the current session: if other biometric data are provided before the timeout expires, it is still possible to get a new certificate and refresh the timeout. If verification is successful, the CASHMA authentication server applies the algorithm to adaptively compute a new timeout of length *Ti*, the expiration time of the session at time $Ti + ti$ 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 $ti + Ti$. Security threats to the CASHMA system have been analyzed both for the enrollment procedure (i.e., initial registration of a user within the system), and the authenticationprocedure itself. We report here only on authentication. The biometric system has been considered as decomposed in functions. For authentication, we considered collection of biometric traits, transmission of (raw) data, features extraction, matching function, tem-plate search and repository management, transmission of the matching score,

decision function, communication of the recognition result (accept/reject decision).

Several relevant threats exist for each function identified. For brevity, we do not consider threats generic of ICT systems and not specific for biometrics (e.g., attacks aimed to Deny of Service, eavesdropping, man-in-the-middle, etc.).

For the collection of biometric traits, we identified sensor spoofing and untrusted device, reuse of residuals to create fake biometric data, impersonation, mimicry and presentation of poor images (for face recognition). For the transmission of (raw) data, we selected fake digital biometric, where an attacker submits false digital biometric data. For the features extraction, we considered insertion of imposter data.

7. Trust Levels and Timeout Computation

The algorithm to evaluate the expiration time of the session executes iteratively on the CASHMA authentication server. It computes a new timeout and consequently the expiration time each time the CASHMA authentication server receives fresh biometric data from a user. Let us assume that the initial phase occurs at time $t0$ when biometric data is acquired and transmitted by the CASHMA application of the user u, and that during the maintenance phase at time $ti>t0$ for any $i=1, \ldots m$ new biometric data is acquired by the CASHMA application of the user u (we assume these data are transmitted to the CASHMA authentication server and lead to successful verification i.e., The steps of the algorithm described hereafter are executed.

To ease the readability of the notation, in the following the user u is often omitted; for example $g(ti) = g(u, ti)$.

7.1 Computation of Trust in the Subsystems

The algorithm starts computing the trust in the subsystems. Intuitively, the subsystem trust level could be simply set to the static value $m(Sk, t)=1-FMR(Sk)$ for each unimodal subsystem Sk and any time t (we assume that information on the subsystems used, including their FMRs, is contained in a repository accessible by the CASHMA Authentication Server).

In the initial phase $m(Sk, t0)$ is set to $1-FMR(Sk)$ for each subsystem Sk used. During the maintenance phase, a pen-alty function is associated to consecutive authentications performed using the same subsystem as follows:

$$\text{penalty}(x, h) = e^{x \cdot h}$$

where x is the number of consecutive authentication at-tempts using the same subsystem and $h>0$ is a parameterused to tune the penalty function. This function increases exponentially; this means that using the same subsystem for several authentications heavily increases the penalty.

The computation of the penalty is the first step or the computation of the subsystem trust level. If the same sub-system is used in consecutive authentications, the subsystem trust level is a multiplication of i) the subsystem trust level $m(Sk, ti-1)$ computed in the previous execution of the algorithm, and ii) the inverse of the penalty function (the higher is the penalty, the lower is the subsystem trust level):

$$m(Sk, ti) = m(Sk, ti-1) \cdot (penalty\ (x, h))^{-1}.$$

Otherwise if the subsystem is used for the first time or in non-consecutive user identity verification, $m(Sk, ti)$ is set to $1-FMR(Sk)$. This computation of the penalty is intuitive but fails if more than one subsystem are compromised (e.g., two fake biometric data can be provided in an alternate way).

7.2 Computation of Trust in the User

As time passes from the most recent user identity verification, the probability that an attacker substituted to the legitimate user increases i.e., the level of trust in the user decreases. This leads us to model the user trust level through time using a function which is asymptotically decreasing towards zero. Among the possible models we selected the function in (1), which: i) asymptotically decreases towards zero; ii) yields $trust(ti-1)$ for $ti=0$; and iii) can be tuned with two parameters which control the delay (s) and the slope (k) with which the trust level decreases over time. Different functions may be preferred under specific conditions or users requirements; in this paper we focus on introducing the protocol, which can be realized also with other functions.

During the initial phase, the user trust level is simply set to $g(t0) = 1$. During the maintenance

phase, the user trust level is computed for each received fresh biometric data. The user trust level at time *ti* is given by:

$$g(t_i) = \frac{(-\arctan((\Delta t_i - s)\cdot k) + \frac{\pi}{2})\cdot trust(t_{i-1})}{-\arctan(-s\cdot k) + \frac{\pi}{2}}. \quad (1)$$

Value *ti*=*ti*-*ti*-1 is the time interval between two data transmissions; *trust*(*ti*-1) instead is the global trust level computed in the previous iteration of the algorithm

7.3Merging User Trust and Subsystems Trust: the Global Trust Level

The global trust level is finally computed combining the user trust level with the subsystem trust level.

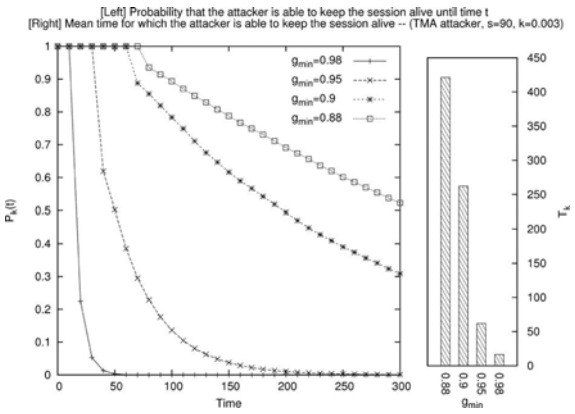
In the initial phase, multiple subsystems may be used to perform an initial strong authentication. Let *n* be the number of different subsystems, the global trust level is firstly computed during the initial phase as follows:

$$trust(t_0) = 1 - \Pi_{k=1,\ldots,n}(1 - m(S_k, t_0)). \quad (2)$$

Equation (2) includes the subsystem trust level of all subsystems used in the initial phase. We remind that for the first authentication *m*(*Sk, t*0) is set to 1-*FMR*(*Sk*). The different subsystems trust levels are combined adopting the *OR*-rule from considering only the false acceptance rate: each subsystem proposes a score, and the combined score is more accurate than the score of each individual subsystem. The first authentication does not consider trust in the user behavior, and only weights the trust in the subsystems. The FNMR is not considered in this computation because it only impact on the reliability of the session, while the user trust level is intended only for security.

Given the user trust level *g*(*ti*) and the subsystem trust level *m*(*Sk, ti*), the global trust level is computed again adopting the *OR*-rule from [2], this time with only two input values. Result is as follows:

$$trust\ (ti) = 1 - (1 - g(ti))\ (1 - m(Sk, ti))$$
$$= g(ti) + m(Sk, ti) - g(ti)\ m(Sk, ti) =$$
$$= g(ti) + (1 - g(ti))\ m(Sk, ti). \quad (3)$$



Effect of the continuous authentication mechanism

8. PROTOTYPE IMPLEMENTATION

The implementation of the CASHMA prototype includes face, voice, iris, fingerprint and online dynamic handwritten signature as biometric traits for biometric kiosks and PCs/laptops, relying on on-board devices when available or pluggable accessories if needed. On smartphones only face and voice recognition are applied: iris recognition was discarded due to the difficulties in acquiring high-quality iris scans using the camera of commercial devices, and handwritten signature recognition is impractical on most of smartphones today available on market (larger displays are required). Finally, fingerprint recognition was discarded because few smartphones include a fingerprint reader. The selected biometric traits (face and voice) suit the need to be acquired transparently for the continuous authentication protocol described.

A prototype of the CASHMA architecture is currently available, providing mobile components to access a secured web application. The client is based on the Adobe Flash technology: it is a specific client, written in Adobe Actions Script 3, able to access and control the on board devices in order to acquire the raw data needed for biometric authentication. In case of smartphones, the CASHMA client component is realized as a native An-droid application (using the Android SDK API 12). Tests were conducted on smart phones Samsung Galaxy S II, HTC Desire, HTC Desire HD and HTC Sensation with OS Android 4.0.x. On average from the executed tests, for the smartphones considered we achieved FMR=2,58% for face recognition and FMR=10% for voice. The dimensions of

biometric data acquired using the considered smart phones and exchanged are approximately 500 KB. As expected from such limited dimension of the data, the acquisition, compression and transmission of these data using the mentioned smart phones did not raise issues on performance or communication bandwidth. In particular, the time required to establish a secure session and transmit the biometric data was deemed sufficiently short to not compromise usability of the mobile device.

Regarding the authentication service, it runs on Apache Tomcat 6 servers and Postgres 8.4 databases. The web services are, instead, realized using the Jersey library (i.e., a JAX-RS/JSR311 Reference Implementation) for building RESTful Web services.

Finally, the example application is a custom portal developed as a Rich Internet Application using SenchaExtJS 4 JavaScript framework, integrating different external online services (e.g. Gmail, Youtube, Twitter, Flickr) made accessible dynamically following the current trust value of the continuous authentication protocol

9. ALGORITHM

The monitor is the central coordinating entity in the architecture that performs the following tasks:

1. it controls the rate at which biometric data is capturedby querying each biometric device and runsthe modality-specific verifier for that sample
2. it combines the verification results from differentmodalities obtained at different times into Psafe, theprobability that the computer system is still *Safe*
3. it periodically communicates Psafe (indirectly, it actually computes and communicates the delay value in jiffies5) to the kernel so that the kernel can appropriately freeze or delay processes.

```
1. double x = current_biometric_classification;
2 .booleanbelow_thresh = (x < threshold);
3
4. if(current->ca_sessid == 0)
5 .do_nothing;
6 .else if(current->ca_sessid ==
ca_global_session)
7 .{
8 .if(syscall is critical &&below_thresh)
9 .freeze yourself;
10. else if(syscall is !critical &&below_thresh)
11. delay yourself by [e(1=S□1=T) □ 1] jiffies
12
13. //!below_thresh )do_nothing;
14 }
15. else if(current-
>ca_sessid<ca_global_session)
16. unconditionally freeze yourself;
```

10. CONCLUSION

The protocol computes adaptive timeouts on the basis of the replacement, override of feature extraction (the attacker is able to interfere with the extraction of the feature set), and exploitation of vulnerabilities of the extraction algorithm. For the matching function, attacks we considered are insertion of imposter data, component replacement, guessing, manipulation of match scores .For template search and repository management, all attacks considered are generic for repositories and not specific to biometric systems. For the trans-mission of the matching score, we considered manipulation of match score. For the decision function, we considered hill climbing (the attacker has access of the matching score, and iteratively submits modified data in an attempt to raise the resulting matching score), system parameter override/modification (the attacker has the possibility to change key parameters as system tolerances in feature matching), component replacement, decision manipulation. For the communication of recognition result, we considered only attacks typical of Internet communications.

REFERENCES:

[1] CASHMA-Context Aware security by Hierarchical Multilevel Architectures, MIUR FIRB2005.

[2] L.Hong,A.Jain, and S.Pankanti,"Can Multibiometrics Improve Performance?", proc.AutoID'99,Summit,NJ,pp.59-64,1999.

[3] BioID,Biometric Authentication as a service (Baas)."BioID press release,3March 2011,https://www.bioid.com.

[4] A.Altinok and M.Turk,"Temporal integration for continuous multi-modal biometrics," Multimodal User Authentication,pp.11-12,2003.

[5] C.Roberts,"Biometric attack vectors and

defences", Computer & Security, vol.26,Issue 1,pp.14-25,2007.

[6] S.Z.Li, and A.K.Jain,Encyclopedia of Biometrics,FirstEdition,Springer Publishing company.Incorporated,2009.

[7] O.Sheyner, J.Haines, S. Jha, R. Lipmann,J.M. Wing, "Automated generation and analysis of attack graph",IEEE Symposium on Security and privacy,pp.273-284,2002.

[8] T.Casey.Threat Agent Library helps idenfy information Security Risks",White Paper, Intel Corporation ,September 2007.

[9]Adobe,Products List,http://www.adobe.com/products[online]

[10] T.F.Dapp,"Growing need for security in online banking:biometrics enjoy remarkable degree of acceptance", Banking & Technology Snapshot DB research,8 February 2012.

[11] A.K.Jain, A. Ross, S. Pankanti, "Biometrics: a tool for information security," IEEE Transactions in Information Forensics and Security, vol.1,pp.125,143,june 2006.

[12] D.M. Nicol, W.H. Sanders, K. S. Trivedi, "Model based evaluation: from dependability to security, "IEEE Trans. Dependable and Secure Computing.

[13] N. Mendes, A.A. Neto, J. Duraes, M. Vieira, H. Madeira, "Assessing and Comparing Security of Web Servers, "IEEE International Symposium on Dependable Computing(PRDC),pp.313-322,2008.

[14] S. Ojala, J. Keinanen, J. Skytta, "Wearable authentication device for transparent login in nomadic applications environment," Proc. 2nd International Conference on Signals, Circuits ansSystems(SCS 2001)pp. 1-6,7-9 Nov.2008.

[15] W. H. Sanders, J. F. Meyer, "Stochastic activity networks : formal definition and concepts", Lectures on formal methods and performance analysis.inc.,pp.315-34,2002.

[16] S. Evans and J. Wallner, "Risk-based security engineering through the eyes of the adversary", in Proc .of the 2005 IEEE Workshop on Information Assurance. United States Military Academy, West Point, NY, June 2005, pp.158-165.

[17] T. Sim, S. Zhang, R. Jankiraman and S. Kumar, " Continuous Verification using Multimodal Biometrics," IEEE Trans. Pattern Analysis and Machine Intelligence, vol.29,no.4,pp.687-700,April 2007..

[18] U. Uludag and A. K. Jain, "Attacks on Biometric Systems: a case study in fingerprints", Proc. SPIE-EI 2004, Security, Stegnography and Water marking of Multimedia Contents VI,pp.622-633,2004.

[19] M. Afzaal, C. DI Sarno, L. Coppolonio, S.D'Antonio, L. Romano, "A Resilient Architecture for Forensic Storage of Events in Critcal Infrastructures", International Symposium on High Assurance Systems engineering,pp.48-55,2012.

[20] M.Cinque, D. Cotroneo, R. Natella, A. Pecchia, "Assessing and improving the effectiveness of logs for the analysis of software faults", International Conference on Depandable Systems and Networks,pp.457-466,2010.