A Continuous Authentication Framework for Securing Internet Services

Ms.Patil Poonam Pramod[1], Prof.Jawalkar Prashant [2]
[1,2] Department ofComputer Engineering
[1,2]JSPMS Bhivrabai Sawant Institute of Technology Research Wagholi, Pune, Maharashtra,India

Abstract*-The session management in Internet services usesusername and password for the security, uncertain logout and unit of user session termination utilizing the good timeouts. So the solution is biometric information is placed in the replacementof username and password during session , however in thismethodology one time verification is considered as abundant, andduring the whole session the identity of user is also thought out asunchanged. biometric development is however the length of thesession timeout could result on the convenience of the service andfuture user fulfillment. In proposing an alternate technique byapplying authentication through continuous user verification byapplying iris application within the sessions of service.So weproposed the Continuous authentication framework for UserIdentity Verification by using iris and fingerprint authentication. Iris recognition uses video camera technology with delicate close to infrared illumination to accumulate pictures of the detail-rich, involved structures of the iris that measure visible outwardly. A secure protocol is characterized for perfectly authentication throughconsistent user check. The protocol decides versatile timeoutstaking under consideration the standard, return and sort ofbiometric info squarely procured from the user.*

Keywords-Iris,CASHMA,Fingerprints

I. INTRODUCTION

In this technology era security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attack s, biometric techniques offer emerging solution for secure and trusted user identity verification, where username and password are replaced by bio-metric traits. Biometrics is the science and technology of determining identity based on physiological and behavioral traits. Biometrics includes retinal scans, finger and handprint recognition, and face recognition, handwriting analysis, voice recognition and Keyboard biometrics. Also, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially in the financial and banking sectors. 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 time when one or more biometric traits may be required. Once the users identity has been verified, the system resources are available for a fixed period of time or until explicit logout from the user. This approach is also susceptible for attack because the identity of the user is constant during the whole session. Suppose, here we consider this simple 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 the user session is active, allowing impostors to impersonate the user and access strictly personal data. In these scenarios, the services where the users are authenticated can be misused easily. The basic solution for this is to use very short session timeouts and request the user to input his login data again and again, but this is not a satisfactory solution. So, to timely identify misuses of computer resources and prevent that, solutions based on iris continuous authentication is proposed, that means turning user verification into a continuous process rather than a onetime authentication. Finally, the use of iris authentication allows credentials to be acquired transparently i.e. without explicitly notifying the user to enter data over and over, which provides guarantee of more security of system than traditional one.

Existing System

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 time when one or more biometric traits may be required.

-Once the users identity has been verified, the system resources are available for a fixed period of time or until explicit logout from the user. This approach is also susceptible for attack because the identity of the user is constant during the whole session. Suppose, here we consider this simple 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 the user session is active, allowing impostors to impersonate the user and access strictly personal data.

-In these scenarios, the services where the users are authenticated can be misused easily. The basic solution for this is to use very short session timeouts and request the user to input his login data again and again, but this is not a satisfactory solution.

-So, to timely identify misuses of computer resources and prevent that, solutions based on bio-metric contin-uous authentication are proposed, that means turning user verification into a continuous process rather than a onetime authentication. Biometrics authentication can depend on multiple biometrics traits. Finally, the use of biometric authentication allows credentials to be acquired transparently i.e. without explicitly notifying the user to enter data over and over, which provides guarantee of more security of system than traditional one.

-In existing work mostly use fingerprint. It is the most economical biometric PC user authentication technique. It is one of the most developed biometrics.

Proposed System

- we proposed iris and fingerprint authentication framework for securing internet services.
_ Iris recognition method uses camera technology. .Irisrecognition is method which is very close to infraredillumination to collect pictures. The structures present inthe iris measured outwardly.
_ These structures are in patterns which are encoded in the form of digital templates. Also the statistical algorithm is used for the identification of a person.
_ Databases of registered templates, measure searched by matcher engines at speeds measured within the several templates per second per central processor, and with remarkably low false match rates.
-A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. A friction ridge is a raised portion of the epidermis on the digits (fingers and toes),consisting of one or more connected ridge units of friction ridge skin.
-An intentional recording of friction ridges is usually made with black printer's ink rolled across a contrasting white background, typically a white card. Friction ridges can also be recorded digitally, usually on a glass plate, using a technique called Live Scan.

Problem Definition

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. Emerging biometric solutions provides substituting username and password with biometric data during session establishment, but in such an approach

still a single shot verification is less sufficient, and the identity of a user is considered permanent during the entire session. A basic solution is to use very short session timeouts and periodically request the user to input his credentials over and over, but this is not a definitive solution and heavily penalizes the service usability and ultimately the satisfaction of users. To timely detect misuses of computer resources and prevent that an unauthorized user maliciously replaces an authorized one, solutions based on multi-modal biometric continuous authentication are proposed, turning user verification into a continuous process rather than a onetime occurrence. To avoid that a single biometric trait is forged, biometrics authentication can rely on multiple bio-metrics traits. In this project we take iris and fingerprint for biometric authentication.

II.REVIEW OF LITERATURE

1.Adversary-driven state-based system security evaluation

Quantitative metrics can aid decision-makers in making informed trade-off decisions. In system-level security decisions, quantitative security metrics allow decision-makers to compare the relative security of different system configurations. To produce model-based quantitative security metrics, we have formally defined and implemented the Adversary View Security Evaluation (ADVISE) method. Our approach is to create an executable state-based security model of a system and an adversary that represents how the adversary is likely to attack the system and the likely results of such an attack. In an ADVISE model, attack steps are precisely defined and organized into an attack execution graph, and an adversary profile captures a particular adversary’s attack preferences and attack goals. We create executable security models that combine information from the attack execution graph, the adversary profile, and the desired security metrics to produce quantitative metrics data. The ADVISE model execution algorithms use the adversary profile and the attack execution graph to simulate how the adversary is likely to attack the system. The adversary selects the best next attack step by evaluating the attractiveness of several attack steps, considering cost, payoff, and the probability of detection. The attack step decision function compares the attractiveness of different attack steps by incorporating the adversary's attack preferences and attack goals. The attack step decision function uses a state look-ahead tree to recursively compute how future attack decisions influence the attractiveness values of the current attack step options. To efficiently produce quantitative model-based security metrics, the ADVISE method has been implemented in atool that facilitates user input of system and adversary data and automatically generates executable models. The tool was used in two case studies that illustrate how to analyze the security of a system using the ADVISE method. The case studies demonstrate the feasibility of ADVISE and provide an example of the type of security analysis that ADVISE enables.

2.Wearable authentication device for transparent login in nomadic applications environment

This paper describes a wearable authentication device for continuous user authentication and transparent login procedure in nomadic applications environment, where users are mobile and current authentication methods are not applicable. The wearable authentication device is a wristband in which the user authentication is done by using the fingerprint and to ensure that the person is wearing the device, it measures continuously his vital signs (skin temperature and heart rate) along with body capacitance and acceleration. By wearing the authentication device, the user can login transparently to any computer simply by approaching it. The prototype of the wearable authentication device was implemented and demonstrated successfully. The user was authenticated with the fingerprint and his presence could be verified continuously by using the skin temperature and the body capacitance. In addition, the heart rate of the user could be obtained from the pulse oximeter output. The received signal strength of the wireless connection offered an inexpensive and simple way to implement the transparent login by estimating the range between the user and a terminal.

3.Quantitative Security Evaluation of a Multi-biometric Authentication System

Biometric authentication systems verify the identity of users by relying on their distinctive traits, like fingerprint, face, iris, signature, voice, etc. Biometrics is commonly perceived as a strong authentication method; in practice several well-known vulnerabilities exist, and security aspects should be carefully considered, especially when it is adopted to secure the access to applications controlling critical systems and infrastructures. In this paper we perform a quantitative security evaluation of the CASHMA multi-biometric authentication system, assessing the security provided by different system configurations against attackers with different capabilities. The analysis is performed using the ADVISE modeling formalism, a formalism for security evaluation that extends attack graphs; it allows to combine information on the system, the attacker, and the metrics of interest to produce quantitative results. The obtained results provide useful insight on the security offered by the different system configurations, and demonstrate the feasibility of the approach to model security threats and countermeasures in real scenarios.

4.Biometric attack vectors and defences

Much has been reported on attempts to fool biometric sensors with false fingerprints, facial overlays and a myriad of other spoofing approaches. Other attack vectors on biometric systems have, however, had less prominence. This paper seeks to present a broader and more practical view of biometric system attack vectors, placing them in the context of a risk-based systems approach to security and outlining defences.

5.Attacks on biometric systems: a case study in fingerprints

In spite of numerous advantages of biometrics-based personal authentication systems over traditional security systems based on token or knowledge, they are vulnerable to attacks that can decrease their security considerably. In this paper, we analyze these attacks in the realm of a fingerprint biometric system. We propose an attack system that uses a hill climbing procedure to synthesize the target minutia templates and evaluate its feasibility with extensive experimental results conducted on a large fingerprint database. Several measures that can be utilized to decrease the probability of such attacks and their ramifications are also presented.

III. SYSTEM ARCHITECTURE

1.Clients :

In this module, each client must register with CASHMA Authentication Server for access the web.

In existing works, each client used fingerprint for their identity. But it can make mistakes with the dryness or dirty of the fingers skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly).

So in this system we have used Iris as well as fingerprint for client identity. This client details with iris and fin-gerprint details are register in CASHMA Authentication Server for client Identity Verification.

2.Cloud Server

This module shows databases of templates that contain the biometric templates of the enrolled users (i.e. Fingerprints and Iris of all the registered users, these are required for user authentication/verification).

3.CASHMA Authentication Server :

This module interacts with clients.

CASHMA authentication server can verify the identity of client by matching the biometric templates present in cloud server.This module work in two phases :

I.Initial Phase :

In this phase, after successful verification of user the CASHMA authentication server provides an authentica-tion certificate to the user with initial session timeout.

II.Maintenance Phase :

In this phase, session timeout is adaptively updated when user identity verification is performed.

4.Web Services :

The web services are the various services that use the CASHMA authentication service and demand the authentication of enrolled 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 authenti-cation service, expressing also their trust threshold.

IV. SYSTEM ANALYSIS

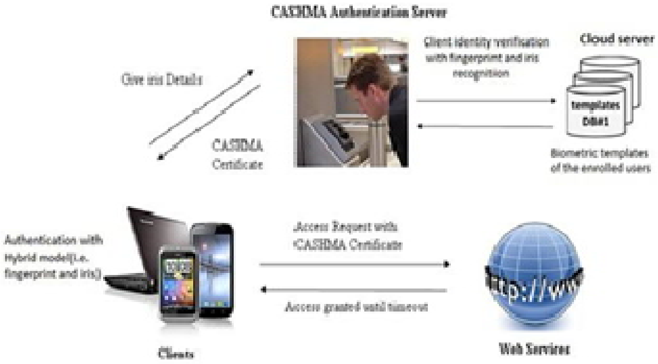
CASHMA Authentication Server
Give iris Details
CASHMA Certificate
Client identity verification with fingerprint and iris recognition
Cloud server
templates DB#1
Biometric templates of the enrolled users
Authentication with Hybrid model(i.e. fingerprint and iris)
Access Request with CASHMA Certificate
Access granted until timeout
Clients
http://ww
Web Services

Fig. 1. Block Diagram of Proposed System

Table I

Comparison Between Proposed And Existing System

POINTS	Proposed System	Existing System (Sec)
Advantages	Very high accuracy.	It is Easy to use.
	Verification time less than 5 sec	It has Small storage space
	It is very difficult to Falsify	it reduce size of the database
Disadvantages	Intrusive	related to criminal identification
	access more memory	make mistakes with age
	Very expensive	demands a large memory space

A. Algorithm

ALGORITHMIC DETAILS:
Input : Multiple Bio-metric traits B={B1,B2}
Output: Continuous identity verification
User first register his details and details of service into Chasma system
Initial Phase:
Step 1: Client send Iris, fingerprint to Biometric (CHASMA) Authentication Server.
Step 2: Biometric (CHASMA) Authentication Server verify Client Identity then send Hybrid Biometric (CHASMA) Certificate Ci to client.
Each certificate will consist of Ci={}
Step 3: Client send access request with Biometric (CHASMA) Certificate to Web service.
Step 4: Web service accept the access request. So Client access web until “timeout” ti.
Maintenance Phase:

Step 5: Client send biometric data to Biometric (CHASMA) Authentication Server.
Step 6: Biometric (CHASMA) Authentication Server verify the Client Identity then send a fresh Biometric (CHASMA) Certificate to client.
Step 7: Now Client send Biometric (CHASMA) Certificate to Web service for update the session timeout Ti(ti+ some constant say t0).

B. Mathematical Model

Give S, a chance to be a framework to such an extent that,
S = {s, Fs, Is, u, C, a, t, o, Ws, X, Y, T,es,ee,etpt,ptpt,ps,pe}

Where,
es=Existing Start time
ee=Existing End time
etpt=Existing total processing time
ptpt=Propose total processing time
ps= Proposed Start time
pe= Proposed End time
S-Proposed System
s- Initial state at T<init> i.e. constructor of a class.
Fs- Fingerprint Signature
Is- Iris Signature
C- CASHMA certificate
u- User
CASHMA Admin
t- Timestamp
ws-web services
o- One Time Password

Equation : $b - a = c, a > b.$
es= System.currentTimeMillis();
ee =System.currentTimeMillis();
etpt = ee-es
ps= System.currentTimeMillis();
pe =System.currentTimeMillis();
ptpt = pe-ps
etpt>ptpt

- Cashma_certificate().

X- Input of System.

- Iris and Fingerprint are input of system

Y- Output of System.

- Web service access with timestamp given by CASHMA admin.

T-Set of serialized ventures to be performed in pipelined machine cycle.

- A special certificate is created for each user which distinguishes the record duplication and provides security.

IV. CONCLUSION

The existing initial one time login verification is inade-quate 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 authenti-cation verification with improves security and usability of user session.

ACKNOWLEDGMENT

This is a great pleasure and immense satisfaction to express my deepest sense of gratitude and thanks to everyone who has directly or indirectly helped me in completing my paper work successfully. I express my gratitude towards project guide Prof. Jawalkar Prashant and Head of Department of

Computer Engineering Dr. G. M. Bhandari, P.G. coordinator Dr. A. C. Lomte, Bhivarabai Sawant Institute Of Technology and Research College Of Engineering, Pune who guided and encouraged me in completing the paper work in scheduled time. I would like to thanks our Principal Dr. T.K.Nagaraj for allowing us to pursue my work in this institute.

REFERENCES

[1] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, Using Continuous Biometric Verification to Protect Interactive Login Sessions, Proc. 21st Ann. Computer Security Applications Conf. (ACSAC 05), pp. 441-450, 2005.

[2] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, Continuous Verication Using Multimodal Biometrics, IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr. 2007.

[3] A. Altinok and M. Turk, Temporal Integration for Continuous Multimodal Biometrics, Proc. Workshop Multimodal User Authenti-cation, pp. 11-12, 2003.

[4] D.M. Nicol, W.H. Sanders, and K.S. Trivedi, Model-Based Evalu-ation: From Dependability to Security, IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1, pp. 48-65, Jan.-Mar. 2004.

[5] Subhash V.Thul, Anurag Rishishwar, NeeteshRaghuwanshi Sum Rule Based Matching Score Level Fusion of Fingerprint and Iris Images for Multimodal Biometrics Identification Feb-2016.

[6] Pradnya M. Shende, Dr. M.V. Sarode Multiple Biometric System Application: Iris And Fingerprint Recognition System March 2016.

[7] PournimaGhanmode, Snehal Mahajan, Pragati Ghodake, BabitaSonare Iris Recognition Based on Extreme Point Identification using Feature Extraction,April 2016.

[8] Mohammad AakifKausar, Gautam Purwar, Rajul Raghuwanshi, Prof. Sachin Deshmukh User Identification Using Iris Scan April 2016.