Incessant and Transparent user Integrity for Protected Internet Services

M. Dhanushya
B. Tech(information technology)
Arasu Engineering College
Kumbakonam,india

S. Raghavi
B. Tech(information technology)
Arasu Engineering College
Kumbakonam,india

T. Senthamizh Chudar
B. Tech(information technology)
Arasu Engineering College
Kumbakonam,india

Mr. Elaiyaraja V M.E..,
Assistant Professor –IT Department
Arasu Engineering College
Kumbakonam, India.

Abstract **- Security of web-based session management is a serious concern, due to the recent increase in the frequency and complexity of cyber-attacks. We present a new attack called the forge-replay attack on username and password systems. It can be launched with easily available Key loggers and APIs for keystroke synthesis. Our experiments from CASHMA authentication achieve alarmingly high error rates compared to zero-effort impostor attacks, which have been the de facto standard for evaluating keystroke-based continuous verification systems. CASHMA authentication provides four state-of-the-art verification methods, three types of keystroke latencies, and 11 matching-pair settings (a key parameter in continuous verification with keystrokes) that we examined in this scheme. In our results, we question the security offered by current keystroke-based continuous verification systems. Additionally, in our experiments, we harnessed virtualization technology to generate of keystroke time slot within a short time span. We point out that virtualization setup such as the one used in our experiments can also be exploited by an attacker to scale and speedup the attack.**

I. 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 termi- nated by an explicit logout or expire after an idle activity period of the user.

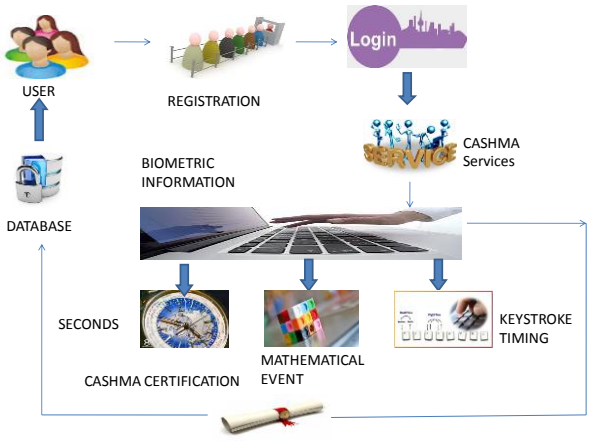
Security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attacks; biometric techniques. offer emerging solution for secure and trusted authentication, where user- name and password are replaced by biometric data. How- ever, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially con- sidering their possible application in the financial and bank- ing sectors.

This paper presents a new approach for user verification and session management that is applied in the context aware security by hierarchical multilevel architectures (CASHMA)) system for secure biometric authentication on the Internet. CASHMA is able to operate securely with any kind of web service, including services with high secu- rity demands as online banking services, and it is intended to be used from different client devices, e.g., smartphones, Desktop PCs or even biometric kiosks placed at the entrance of secure areas. Depending on the preferences and require- ments of the owner of the web service, the CASHMA authentication service can complement a traditional authen- tication 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) multi-modal biometric authentication protocol, which adap- tively 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 CASHMA context, each subsystem comprises all the hardware/software elements necessary to acquire and verify the authenticity of one bio- metric 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 sub- system 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.

Exemplary runs carried out using Matlab are reported, and a quantitative model-based security analysis of the protocol is performed combining the stochastic activity networks and ADversary VIew Security Eval- uation formalisms.

The driving principles behind our protocol were briefly discussed in the short paper , together with minor quali- tative evaluations. This paper extends both in the design and the evaluation parts, by providing an in-depth description of the protocol and presenting extensive qualita- tive and quantitative analysis.

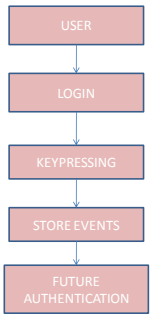


II. MODULES

1. Keystroke Dynamics
2. CASHMA Authentication
3. Misspelt Word
4. Continuous Verification
5. Keystroke Timing

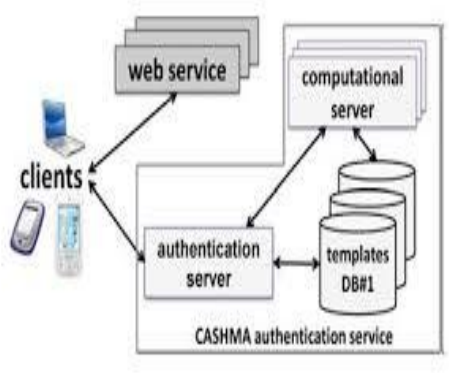
Keystroke Dynamics

FLOW CHART

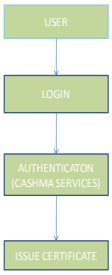


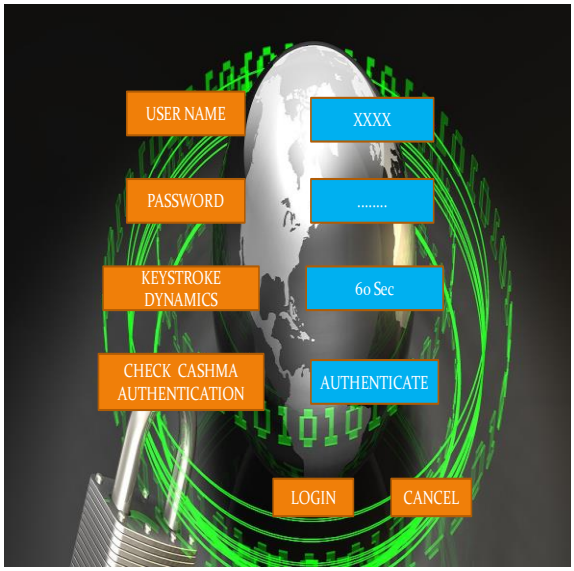
The keystroke rhythms of a user are measured to develop a unique biometric template of the users typing pattern for future authentication. It measurements available from almost every keyboard can be stored even recorded to Dwell timing of key pressed and the time between "key up" and the right next "key down". The saved keystroke timing data is then processed through a unique and specific neural algorithm, which determines a primary pattern for future comparison.

CASHMA Authentication



FLOW CHART



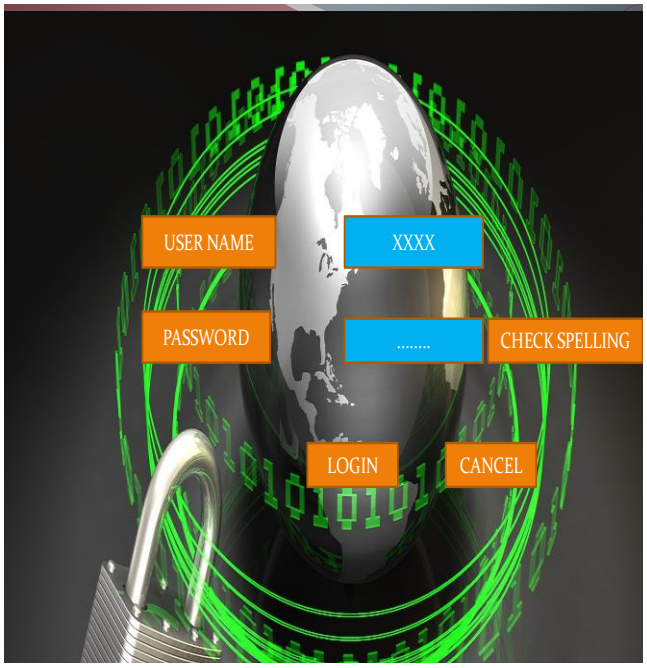


Password collection by keystroke and related malware is increasing at an alarming rate. The attacker can make them stop working heuristics to impute missing latency values or only selected latencies from a victim, to generate desired text or system commands. It provides a trusted path to the user for obtaining authentication credentials. Although generally stateless, it can store

temporary session keys and may optionally act as a password manager. This page could be completely under the control of spyware, or it could be controlled by an online site in-the-middle.

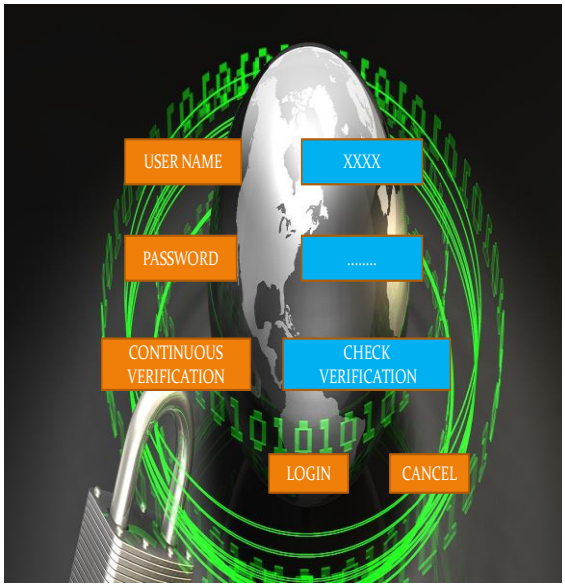
Misspelt Word

FLOW CHART



Calculate the rate of Misspelt word when the user types the text wrongly. This performs the step when the number of times each of the words whose misspellings are being identified was found in the entire text body is counted and recorded. The attacking can be found then this recorded rate match with the original latency of the text. The attack can be found and mitigated when the calculated score does not match with the original record of data.

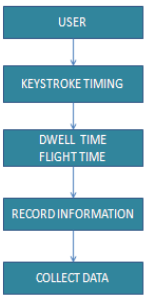
Continuous Verification

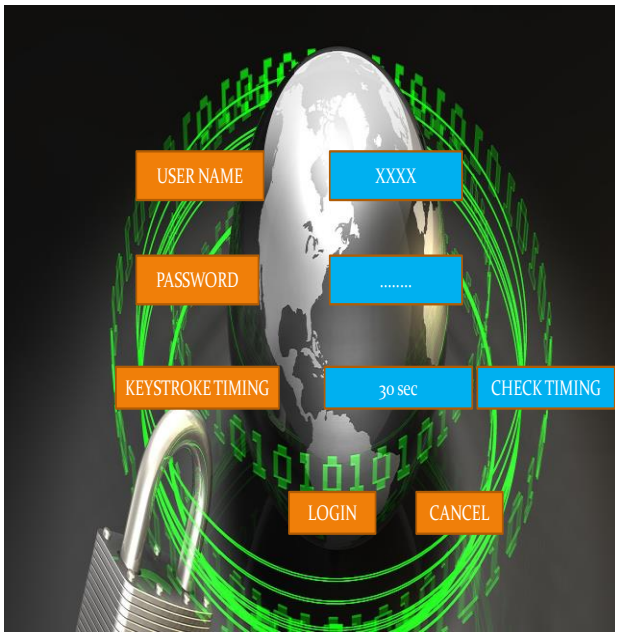


It provides a perfect match (or mis-match) between the continuous verification system and the authentication. Each of the keystrokes is calculated as per the system de-signed. Continuous verification, some keystrokes typed during the verification phase may not have reference signatures in the template. It happen because the enrollment text used for building the template may not have all the letter pairs present in the 26-by-26 matrix. This problem can be resolved by performing verification using letter pairs that are common to the template and the verification text.

Keystroke Timing

FLOW CHART





We present the keystroke timing information, if the typed the text this is text, the attacker records a series of timestamps (time when was pressed), (time when was released), and so on. The participants were allowed to make spelling mistakes, typographical errors and if they chose, could correct them using Backspace or Delete keys. The key-stroke data collection software provided for typing copy and self texts. The results additionally show that effective keystroke forgeries can be created with a) as low as 20 to 100 characters of text and keystroke timing information.

III. CONCLUSION

We exploited the novel possibility introduced by biometrics to define a protocol for continuous authentication that improves security and usability of user session. The proto- col computes adaptive timeouts on the basis of the trust posed in the user activity and in the quality and kind of bio- metric data acquired transparently through monitoring in background the user's actions.

REFERENCES

[1] CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.
[2] L. Hong, A. Jain, and S. Pankanti, "Can Multibiometrics Improve Performance?" Proc. Workshop on Automatic Identification Advances Technologies (AutoID '99) Summit, pp. 59-64, 1999.
[3] S. Ojala, J. Keinanen, and J. Skytta, "Wearable Authentication Device for TransparentLogin in Nomadic Applications Environment," Proc. Second Int'l Conf. Signals, Circuits and Systems (SCS '08), pp. 1-6, Nov. 2008.
[4] BioID "Biometric Authentication as a Service (BaaS)," BioID Press Release, https://www.bioid.com, Mar. 2011.
[5] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr.

PROFILE

Mr.V.ELAIYARAJA working as Assistant Professor in **B.TECH(IT)** Arasu Engineering College approved by AICTE and Anna University Chennai. He was vast experience in Computer science Engineering.

Miss.M.DHANUSHYA is a student of **B.TECH (IT)** at Arasu Engineering College approved by AICTE and Anna University Chennai. Her areas of interest are Networking and Cloud computing,Database management systems.

Miss.S.RAGHAVI is a student of **B.TECH (IT)** at Arasu Engineering College approved by AICTE and Anna University Chennai. Her areas of interest are Network Security and Distributed systems.

Miss.T.SENTHAMIZH CHUDAR is a student of **B.TECH (IT)** at Arasu Engineering College approved by AICTE and Anna University Chennai. Her areas of interest are Networking and Distributed systems.