Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-9, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Continuous and Biometric Authentication for Secure Internet Services

Ratna Wagh[1] & Prof. G. S. Deokate[2]
[1]Student, ME Computer, SPCOE, Department Of Computer Engineering, Otur
[2]Assistant Professor, SPCOE, Department Of Computer Engineering, Otur

Abstract*: Typically, biometric systems authenticate the user at a particular moment in time, granting or denying access to resources for the complete session. This model of authentication does not appropriately address environments where a different individual may take over a system from the original user (either willingly or otherwise). We propose a multimodal system that performs authentication continuously by integrating information temporally as well as across modalities. Such continuous authentication provides ongoing (rather than onetime) verification and can easily be coupled with another system for dynamically adjusting access to privileges accordingly. We present an initial approach for temporal integration based on uncertainty propagation over time for estimating channel output distribution from recent history, and classification with uncertainty. Our method operates continuously by computing expected values as a function of time differences. Our preliminary experiments show that temporal information improves authentication accuracy. These empirical results are promising and justify further investigation.*

Keywords*: Security, Web Servers, Mobile Environments, Authentication.*

1. Introduction

USER authentication is extremely important for computer and network system security. Currently, knowledge-based methods (e.g., passwords) and token based methods(e.g., smart cards) are the most popular approaches. However ,these methods have a number of security flaws. For example, passwords can be easily shared, stolen, and forgotten. Similarly, smart cards can be shared, stolen, duplicated, or lost. To circumvent these issues, a number of login authentication methods, including textual , graphical passwords and biometric authentication, have been utilized. All of the above login methods share a common problem, namely, they authenticate a user only at the initial log-in session and do not reauthenticate a user until the user logs out. Anyone can access the system resources if the initial user does not properly log out or the user leaves the workstation unattended to take a short break without logging out. To resolve this problem, the system must continuously monitor and authenticate the user after the initial login session. In order to achieve this objective, we need to develop robust, reliable, and user-friendly methods for continuous user authentication. It is desirable that the resulting system has good usability by authenticating a user without his active cooperation.

Continuous Authentication is essential in online examinations where the user has to be continuously verified during the entire session. It can be used in many real time applications, when accessing a secure file or during the online banking transactions where there is need of highly secure continuous verification of the user. A number of biometric characteristics exist and are used in various applications. Each biometric has its own strengths and weaknesses, and the choice depends on the application. Some of the commonly used hard biometrics are Face, Hand geometry, Fingerprint, Iris. Soft biometrics include Keystroke, Voice, Colour of the clothing, Facial colour etc [1,2]. A single biometric trait (unimodal technique) is not sufficient to authenticate a user continuously because the system sometimes cannot observe the biometric information. To address the limitations of single biometrics, using multimodal biometrics is a good solution. It is the combination of two or more biometric traits to raise systems security and reliability. Multimodal has several advantage over unimodal. Combining the results obtained by different biometric traits by an effective fusion scheme can significantly improve the overall accuracy of the biometric system.

Multimodal system increases the number of individuals that can enroll. It provides resistance against spoofing. The proposed work includes Sclera and Fingerprint as their Multimodal biometric traits for continuous authentication of the user. The blood vessel structure of the sclera is unique to each person, and it can be remotely obtained non intrusively in the visible wavelengths.

2. Related Work

Using continuous biometric verification to protect interactive login sessions: In this paper we describe the theory, architecture, implementation, and performance of a multimodal passive biometric verification system that continually verifies the

presence/participation of a logged-in user. We assume that the user logged in using strong authentication prior to the starting of the continuous verification process. While the implementation described in the paper combines a digital camera-based face verification with a mouse-based fingerprint reader, the architecture is generic enough to accommodate additional biometric devices with different accuracy of classifying a given user from an imposter. The main thrust of our work is to build a multimodal biometric feedback mechanism into the operating system so that verification failure can automatically lock up the computer within some estimate of the time it takes to subvert the computer. This must be done with low false positives in order to realize a usable system.

Continuous Verification Using Multimodal Biometrics: Conventional verification systems, such as those controlling access to a secure room, do not usually require the user to reauthenticate himself for continued access to the protected resource. This may not be sufficient for high-security environments in which the protected resource needs to be continuously monitored for unauthorized use. In such cases, continuous verification is needed. In this paper, we present the theory, architecture, implementation, and performance of a multimodal biometrics verification system that continuously verifies the presence of a logged-in user. Two modalities are currently used - face and fingerprint - but our theory can be readily extended to include more modalities. We show that continuous verification imposes additional requirements on multimodal fusion when compared to conventional verification systems. We also argue that the usual performance metrics of false accept and false reject rates are insufficient yardsticks for continuous verification and propose new metrics against which we benchmark our system.

Temporal integration for continuous multimodal biometrics: Typically, biometric systems authenticate the user at a particular moment in time, granting or denying access to resources for the complete session. This model of authentication does not appropriately address environments where a different individual may take over a system from the original user (either willingly or otherwise). We propose a multimodal system that performs authentication continuously by integrating information temporally as well as across modalities. Such continuous authentication provides ongoing (rather than onetime) verification and can easily be coupled with another system for dynamically adjusting access to privileges accordingly. We present an initial approach for temporal integration based on uncertainty propagation over time for estimating channel output distribution from recent history, and classification with uncertainty. Our method operates continuously by computing expected values as a function of time differences.

Model-based evaluation: from dependability to security: The development of techniques for quantitative, model-based evaluation of computer system dependability has a long and rich history. A wide array of model-based evaluation techniques is now available, ranging from combinatorial methods, which are useful for quick, rough-cut analyses, to state-based methods, such as Markov reward models, and detailed, discrete-event simulation. The use of quantitative techniques for security evaluation is much less common, and has typically taken the form of formal analysis of small parts of an overall design, or experimental red team-based approaches. Alone, neither of these approaches is fully satisfactory, and we argue that there is much to be gained through the development of a sound model-based methodology for quantifying the security one can expect from a particular design. In this work, we survey existing model-based techniques for evaluating system dependability, and summarize how they are now being extended to evaluate system security. We find that many techniques from dependability evaluation can be applied in the security domain, but that significant challenges remain, largely due to fundamental differences between the accidental nature of the faults commonly assumed in dependability evaluation, and the intentional, human nature of cyber attacks.

Automated generation and analysis of attack graphs: An integral part of modeling the global view of network security is constructing attack graphs. Manual attack graph construction is tedious, error-prone, and impractical for attack graphs larger than a hundred nodes. In this paper we present an automated technique for generating and analyzing attack graphs. We base our technique on symbolic model checking algorithms, letting us construct attack graphs automatically and efficiently. We also describe two analyses to help decide which attacks would be most cost-effective to guard against.

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 a tool 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.The ADVISE method aggregates security-relevant information about a system and its adversaries to produce a quantitative security analysis useful for holistic system security decisions. System architects can use ADVISE models to compare the security strength of system architecture variants and analyze the threats posed by different adversaries.

3. Proposed Work

A. Description

The proposed work uses multimodal biometrics for continuous authentication namely sclera blood vein pattern and fingerprint. For initial log in uses sclera blood veins as it is unique to each individual and it is more ac-curate than any other biometric. The experimental re-sults show that sclera recognition is a promising new biometrics for positive human ID[7]. A new method for sclera segmentation which works for both colour and grayscale images is proposed and, we designed a Gabor wavelet-based sclera pattern enhancement method to emphasize and binarize the sclera vessel patterns [6].Then continuously verifying the user by the bio-metric mouse.

B. Multimodal Biometrics

There has been a good deal of research in recent years on integrating multiple modalities to identify or authenticate a user. In such a multimodal biometric system, the method of integration is very important, as the accuracy of a strong biometric could suffer when integrated with a weaker biometric. Interestingly, most accurate biometrics (iris scan, fingerprint, DNA matching and the like) are either lengthy procedures in collection or verification, or they are intrusive and cannot be performed frequently. A static multimodal system can only use such accurate indicators once they are observed here.

C. Temporal Integration

There are several challenges for temporal ("horizontal") integration of a multimodal authentication system. First, as mentioned in the introduction, individual biometric channels cannot always provide simultaneous observations. One channel might provide information at a much higher frequency than another channel. Second, some channels might only provide sporadic observations over time. For example, we could not expect the user to provide a fingerprint at certain times. Third, for sporadic channels alone, temporal integration could be useless or statistically meaningless, if not impossible, to formulate, since there might be unexpectedly long intervals between observations. Fourth, the system should provide a way of making decisions during time intervals even if none of the individual channels provide any observations in that instant. For example, if we made observations δ milliseconds ago, then the system should be able to make decisions based on recent observations as we would not expect the user to be away in such a short interval. Our method addresses all of these challenges. Logically, we have the choice of first integrating temporally or over channels (horizontally or vertically). If we first integrate over channels, then the problem is equivalent to temporal integration using a single biometric channel. On the other hand, integrating temporally first enables us to work with asynchronous biometric channels, since within some neighborhood in time of an observation we will have very good estimates from that observation. For making decisions in the absence of observations at a given point in time, we use expected values of observations from channels with varying degree of uncertainty. Perhaps the best approach, but also the most complex to formulate, is to integrate in both directions (across channels and across time) simultaneously, rather than sequentially.

D. Objectives

State Of The Art: Determine the state of the art on solutions for continuous authentication in distributed and mobile systems. Consider in particular the case of a user holding a mobile device (e.g., a smart phone) which accesses an Internet service.

E. Challenges and Opportunities

Considering separately uni-modal and multi-modal biometrics systems, identify:

1. The main challenges of applying a continuous authentication approach for Internet services using a mobile device in heterogeneous environments (e.g., noisy environments as train stations or marketplace), and
2. The main opportunities offered by such approach.

4. 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. In a multi-modal biometric verification system is designed and developed to detect the physical presence of the user logged in a computer. The proposed approach assumes that first the user logs in using a strong authentication procedure, then a continuous verification process is started based on multi- modal biometric. Verification failure together with a conservative estimate of the time required to subvert the computer can automatically lock it up. Similarly, in a multi- modal biometric verification system is presented, which 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.

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 which depends on the availability of past observations: based on the assumption that as time passes, the confidence in the acquired (aging) values decreases. the paper applies a degeneracy function that measures the uncertainty of the score computed by the verification function. In, despite the focus is not on continuous authentication, an automatic tuning of decision parameters (thresholds) for sequential multi-biometric score fusion is presented: the principle to achieve multimodality is to consider monomodal biometric subsystems sequentially.

5. Conclusion

We have introduced a new model for temporal integration in biometric user authentication and developed an initial method for a continuous authentication system. Our temporal integration method depends on the availability of past observations, which makes the length of relevant history an important heuristic. Another important design choice is the degeneracy function. The existence of a cross-over point in the history suggests further investigation of the degeneracy.

We have shown on simulated data that our preliminary system can provide continuous authentication results which are consistently better than individual components of the system. Clearly, gathering a true multimodal database is very important for continued work in this field. When the history length is set to 0, the system ignores temporal integration and degenerates into a multimodal system. Although our approach attempts to minimize the filtering effect of false positives and false negatives, our temporal integration method would suffer from this smoothing behavior to some degree as it stands. The net effect of this behavior is integration of positive decisions, as well as negative ones, as expected.

6. Acknowledgement

I express my sincere thanks to my project guide Prof. G. S. Deokate who always being with presence & constant, constructive criticism to made this paper. I would also like to thank all the staff of computer department for their valuable guidance, suggestion and support through the paper work, who has given co-operation for the project with personal attention. Above all I express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during paper work.

7. References

[1] Sathish Kumar M., Karrunakaran C.M., Vikram M., "Process facilitated enhancement of lipase production from germinated maize oil in Bacillus spp. using various feeding strategies", *Australian Journal of Basic and Applied Sciences, ISSN* : 1991-8178, 4(10) (2010) pp. 4958-4961.

[2] CASHMA - Context Aware Security by Hierarchical Multilevel Architectures, *MIUR FIRB* 2005

[3] Kaliyamurthie K.P., Parameswari D., Udayakumar R., "QOS aware privacy preserving location monitoring in wireless sensor network", *Indian Journal of Science and Technology, ISSN* : 0974-6846, 6(S5) (2013) pp.4648-4652.

[4] L. Hong, A. Jain, and S. Pankanti, "Can Multibiometrics Improve Per- formance?," *Proc. AutoID'99, Summit, NJ*, pp. 59–64, 1999.

[5] Sharmila D., Muthusamy P., "Removal of heavy metal from industrial effluent using bio adsorbents (Camellia sinensis)", *Journal of Chemical and Pharmaceutical Research, ISSN* : 0975 – 7384, 5(2) (2013) pp.10-13.

[6] S. Ojala, J. Keinanen, J. Skytta, "Wearable authentication device for transparent login in nomadic applications environment," *Proc. 2nd International Conference on Signals, Circuits and Systems* (SCS 2008), pp. 1-6, 7-9 Nov. 2008 phase directly on the client device)

[7] Udayakumar R., Khanaa V., Saravanan T., Saritha G., "Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction", *Middle - East Journal of Scientific Research, ISSN* : 1990-9233, 16(12) (2013) pp.1781-1785.
[8] Kalaiselvi V.S., Prabhu K., Ramesh M., Venkatesan V., "The association of serum osteocalcin with the bone mineral density in post menopausal women",*Journal of Clinical and Diagnostic Research, ISSN* : 0973 - 709X, 7(5) (2013) pp.814-816.
[9] Kulanthaivel L., Srinivasan P., Shanmugam V., Periyasamy B.M., "Therapeutic efficacy of kaempferol against AFB1 induced experimental hepatocarcinogenesis with reference to lipid peroxidation, antioxidants and biotransformation enzymes", *Biomedicine and Preventive Nutrition, ISSN* : 2210-5239, 2(4) (2012) pp.252-259.
[10] Sangeetha Rajagurusamy, "Analysis of Work study in An Automobile Company", *International Journal of Innovative Research in Science, Engineering and Technology, ISSN*: 2319-8753 , pp 5622-5631,Vol. 2, Issue 10, October 2013.
[11] V.G.Vijaya, "Analysis of Rigid Flange Couplings", *International Journal of Innovative Research in Science, Engineering and Technology ,ISSN*: 2319- 8753 , pp 7118-7126,Vol. 2, Issue 12, December 2013.