Approaches and Issues in Location-Aware Continuous Authentication

Stan Kurkovsky and Ewa Syta
Department of Computer Science, Central Connecticut State University, USA
kurkovskysta@ccsu.edu, sytaewa@ccsu.edu

***Abstract*—Convergence of technologies enabling physical and information security makes it possible to combine the features of location-aware and continuous authentication in a single system. We discuss the design of a location-aware continuous authentication system and discuss different implementation approaches that would strike a balance between usability and security of such a system. Issues of location privacy arising from using such systems are also discussed.**

Keywords-continuous authentication; location awareness

I. INTRODUCTION

Today, there is a clear trend of convergence between physical and information security. On the one hand, it is easy to envision a scenario when access to sensitive information resources may often be prevented by securing the physical location of a computer terminal. Alternatively, physical access to a secure room or building could be gained by breaking into a computerized security system. On the other hand, technologies used to monitor and secure both physical and information access are also converging and becoming one and the same. For example, a CCTV system used for monitoring a secure location is more likely to record its video feed to a file on a networked server rather than onto physical videotape; such systems could use computational techniques instead of the security personnel to identify and track people's faces and objects or identify unusual movement patterns. A physical access control system that uses key fobs or smartcards is likely to verify user access privileges at every access attempt by connecting to a corresponding authentication service on a computer network.

Increasing complexity and distributed nature of modern information systems leads to a growing number of vulnerabilities, which, combined with an exponentially growing number of security incidents, may bring a new set of requirements to user authentication mechanisms. Traditional static authentication systems provide only a point-of-entry authentication, while the user's identity is not verified at any subsequent point during the session. In many situations, such a static authentication mechanism may not be acceptable. Convergence of technologies used to implement physical and information security could enable a new approach, location-aware continuous authentication, which would provide a mechanism to verify the presence of a valid authenticated user throughout the entire session and would also allow the users to move freely from one terminal to the next while maintaining their login state.

In this paper we discuss different approaches to implementing location-aware continuous authentication systems. We begin by reviewing existing work in both location-aware and continuous authentication and present a set of requirements for an authentication system that would successfully combine these two capabilities. There is a substantial amount of current research on using biometric systems for continuous authentication; therefore, we analyze the suitability of this authentication modality for location-aware applications. Finally, we discuss the issues of privacy in location-aware continuous authentication applications.

II. CONTINUOUS AUTHENTICATION

Authentication is the process of verifying the user's identity to ensure integrity, confidentiality, and availability of an information system. A traditional static authentication process yields a binary decision about granting access to the system or a resource. Authentication process involves three phases: enrollment, presentation and evaluation. Enrolment requires users to provide information about them, which is then stored permanently within the authentication system. This information may vary depending on the authentication factor(s) used by the system; these factors include knowledge (e.g. a password or a passphrase), possession (e.g. an access card or a key fob), or biometrics (e.g. an iris scan or a fingerprint). Presentation is a process of acquiring a new authentication sample every time the user's identity needs to be verified. Evaluation involves comparing the newly acquired authentication sample with the one recorded during the enrollment phase and making a decision whether access should be granted.

As shown in Figure 1, continuous authentication incorporates the static process of point-of-entry authentication and adds an extra layer of protection by periodically verifying the presence of a valid user during an active session after access to the secured resources has been granted. A typical continuous authentication system uses several authentication factors to increase the level of security and to lessen its intrusiveness. For example, knowledge-based factors, such as a password, can be used for point-of-entry authentication. However, all subsequent verifications of the user's identity should be as unobtrusive as possible to minimize the chances of disrupting the user's work. For example, querying the presence of an access card or using face recognition algorithms to analyze periodically taken snapshots of the user could fulfill such requirements. Consequently, we could distinguish between the *active* stage of continuous authentication that requires actions of the user,

and a *passive* stage, during which user verification is performed without disrupting the user's activity.

In a continuous authentication process, the presentation and evaluation phases are repeated continuously during the passive stage. At any time when the user's identity cannot be positively verified, their access rights are revoked. Consequently, continuous authentication process reverts back to its active stage requiring an explicit intervention from the user.

While authentication is a process of verifying that a particular user trying to log in with a given set of credentials is the actual user to whom these credentials have been assigned, access control is a process used to verify that a particular user is allowed to access a specific resource [21]. Users are matched to resources through a set of authorizations specified in access control policies. Authentication and access control are closely related to each other: access control matches access requests of authenticated users with existing authorizations; access is granted if a match is found, otherwise it is denied. In role-based access control (RBAC), authorizations are not associated with individual users. Instead, users can be assigned one or more roles, which are used as intermediaries between users and permissions. In RBAC, permission is a pairing of a resource or service with an action that can be performed on it.

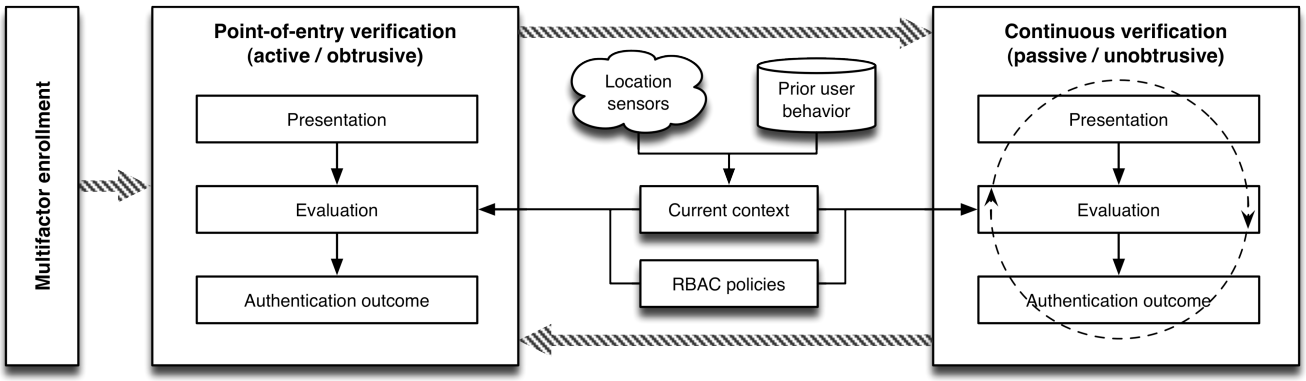

Figure 1. Location-aware continuous authentication scheme

III. . LOCATION-AWARE AUTHENTICATION

In an enterprise environment workers may log in to different workstations at various locations, access enterprise resources from their mobile devices or from remotely connected computers. While such a distributed nature of information access increases the availability of information resources and services, it may have an adverse impact on security of that information and services. It is possible to envision that users who ordinarily would have access to a particular information resource or service from within their normal workplace, may have to be restricted from accessing these resources if this can potentially compromise these resources due to some environmental factors. Examples of such situations may include accessing a resource using the workstation in the office of another employee who does not have access rights to these resources; accessing a resource using a secure laptop, but from a location that can be compromised, e.g. a crowded cafe. In such cases, location information may be a decisive factor in the determining which access control policy is to be applied.

User authentication techniques and access control mechanisms are both well-established areas. However, there are a limited number of recent research reports on incorporating elements of location awareness into authentication and access control.

Using location information to facilitate authentication was first proposed by Denning and MacDoran [10]. In this model, traditional static authentication mechanisms are augmented and strengthened by the user's location information obtained with the help of GPS (Global Positioning System). An additional layer of security is added by verifying that the user's claimed location is the same as their actual location. Bardram et al [2] extend Denning's work and introduce the concept of proximity-based login, which "allows users to be authenticated on a device simply by approaching it physically." Additionally, this concept embraces the principles of context-awareness and integrates them with multi-factor authentication. User location, a crucial component in the user context, is then integrated with the three classical user authentication factors: knowledge, possession, and biometric factors.

Traditional RBAC model can be extended to include location awareness into the definition of roles [19]. GEO-RBAC operates with spatial roles, which combine the geometric features of the user's current location with their role [8]. In GEO-RBAC, spatial roles can be automatically enabled or disabled when the user enters or leaves a particular location. Currently enabled spatial roles then can be activated if the user chooses to do so. Such roles are automatically deactivated if the user leaves the location associated with that role. Despite a substantial amount of conceptual research on this topic, there are many open

research questions associated with GEO-RBAC. For example, it is unclear what happens if there are two or more conflicting roles whose spatial extents overlap or two or more authorized users try to activate the same spatial role at the same time. More generally, GEO-RBAC leaves many unanswered questions related to change in the user environment, characteristics of the user, or the corresponding role. GEO-RBAC could be extended to use events in order to make it more suitable to respond to changes in the environment and the related context [3]. Currently, the process of role enabling and activation is an implicit representation of an event corresponding to a change in the user location. Changing location is just one example of such a change; an access control model must be flexible enough to incorporate dynamic changes not only in location, but in other context variables as well, such as presence of other users, date and time, and past user history.

IV. Requirements for Location-Aware Continuous Authentication

As shown in Figure 1, in addition to the traditional requirements of any authentication system, location-aware authentication must have a number of special features in order to maintain the balance between its usability and the security guarantees it provides:

- Location-sensing: must be able to capture and record current user location;
- Location-aware: make authentication and access control decisions based on the user's current and past location.

Continuous authentication imposes a number of additional requirements, primarily related to the usability of the system:

- Unobtrusive: users should find it simple and easy to use;
- Transparent: with the exception of point-of-entry, authentication process should occur without an explicit interaction with the user;
- Continuous: presence of an authenticated user must be ensured at all times.

A broad range of approaches has been proposed to implement the concept of continuous authentication in an unobtrusive fashion. Face recognition using the images obtained by a trusted camera and performed at regular intervals is one of the more common methods to perform continuous authentication. Such a method has been proposed to authenticate pilots and other personnel authorized to operate commercial aircraft [7]. Non-biometric aspects of user behavior, such as keystrokes, mouse movements, etc., can also be continuously recorded and analyzed. Continuous analysis of temporal patterns in user behavior and detecting anomalies in these patterns has been proposed to detect possible intrusions into a computer system [22].

While the vast majority of research on continuous authentication focuses on using physical or behavioral biometrics, spatial information in location-aware authentication is typically collected using GPS [10] or RFID (Radio Frequency Identification) [14] technologies.

The greatest advantage of using RFID technology is that it can satisfy the requirements of both location-aware and continuous authentication. RFID sensors can easily collect location information and identity of the users whose RFID tags are present nearby. At the same time, RFID technology provides an unobtrusive means for periodic communication between the tags and readers that can occur without requiring a user interaction,

One of the main perceived disadvantages of using a possession-based authentication method such as RFID is that it provides a lower level of assurance compared with biometric authentication. Unless the token used in possession-based authentication is implanted in the human body, it can be easily lost or stolen. However, there is a growing criticism that many biometric samples can be easily forged, especially those that are less intrusive to acquire [9,15]. For example, an intruder could obtain a photograph of a valid user and hold it in front of the camera used to obtain a biometric sample for continuous user authentication. To a certain extent, this flaw can be addressed by combining multiple biometric modalities and/or by using multiple authentication factors to verify the presence of a valid user. Although a unimodal or a single-factor system could be more cost-efficient, multimodal/multifactor systems provide a significantly higher reliability of the decisions made by the authentication system. Finally, an authentication system that uses multiple authentication factors and/or multiple biometric modalities provides a higher degree of assurance because it is much more difficult to forge several authentication samples or fraudulently obtain knowledge-, possession-, and biometric-based samples at the same time.

V. Are Biometrics a Good Fit for Location-Aware Authentication?

Single-modality and multimodal biometrics have been shown as highly reliable methods to implement both point-of-entry and continuous authentication systems [23]. However, deployment of biometrics-based authentication systems is challenging due to many unresolved issues related to user privacy and related legal concerns [18], relatively low user acceptance [12] and the tradeoff between the intrusiveness of the system and the degree of accuracy it provides [20]. While biometric authentication has a demonstrated record of being applied in continuous authentication, there are a number of challenges related to its usability in location-aware authentication applications.

A. Biometric-based Authentication Implementations

Azzini et al. [1] propose using multimodal biometrics for continuous authentication. This approach allows combining multiple biometric authentication samples obtained from multiple sensors, as well as combining different biometric matching algorithms. In particular, this architecture was tested by implementing authentication using two kinds of biometric samples: face snapshots and fingerprints. A fuzzy controller processes a continuous feed of biometric samples (face snapshots) and produces a quantified measure of trust in user identification. Fingerprint recognition is used for point-of-entry authentication or whenever the fuzzy

controller produces an output with the value of trust below an acceptable level.

HUMABIO is a conceptual generalized system for biometric authentication with a special emphasis on unobtrusiveness described by Damousis et al. [9]. This system was also designed to prevent potential attackers from feeding physically duplicated or forged biometric samples into the system, e.g. holding photographs of rightful users in front of a camera, using a voice recording to obtain a speech sample, or using a forged fingerprint. Consequently, HUMABIO makes a substantial effort to verify the continued aliveness of the authenticated user using face, gait and voice recognition among others.

Brosso et al. [5] describe an authentication mechanism based on a context-aware approach. All details of user interaction with the computer system are analyzed and recorded to capture the information of who (which user), where (using which terminal or device), when (a time stamp), performed what action (a specific function invoked in the software system) and why they did that (any repetitiveness in the user actions). Using a neural network, the described authentication system learns a set behavior patterns of every valid user in various contexts. In a continuous authentication phase, this system is claimed to be capable of discerning the deviations from normal user behavioral patterns with a given degree of certainty.

Feasibility of haptic-based biometrics for continuous authentication is discussed by Orozco et al [17]. Haptic-based applications, such as tele-operation or tele-training, are well suited to continuously gather a range of biometric parameters including velocity, position, torque and force. In such haptic-based applications the user is typically required to continuously manipulate a physical object, which essentially precludes any significant changes in the user location. Consequently, haptic technology may not be the best candidate to implement continuous authentication with location-awareness features.

Niinuma et al [16] propose using soft biometric traits, such as the color of the user's clothes or their facial skin, in continuous authentication. In this approach, point-of-entry authentication is achieved using a combination of more traditional methods, such as password and face recognition. During the point-of-entry phase, soft biometric authentication samples are acquired and used continuously throughout the session. This design has been shown to have a high tolerance to the user's posture, which could make it suitable for location-aware continuous authentication systems, where users are allowed to move around freely.

B. Discussion

One of the main drawbacks of continuous authentication systems based on face recognition is that they require the users to be in the field of view of the camera. Depending on the frequency with which a face snapshot is taken, simply turning the head away from the camera for an instant may cause the authentication system to switch into an active stage (point-of-entry mode) and subject the user to an obtrusive form of authentication.

No biometric system can produce a binary authentication decision; instead such systems produce an evaluation metric representing how closely the acquired sample matches that provided during enrollment. Therefore, it is often required to set a certain acceptance threshold representing the balance between the accuracy of the system and its tolerance to false rejections and false acceptances. Compounded with the requirement of some biometric systems for the user to be in the camera's field of view, it may be especially challenging to find an acceptance threshold without compromising the quality of recognition and yet making the system unobtrusive.

Furthermore, a biometric system that requires an active user interaction with various sensors to collect authentication samples may not be an ideal candidate for location-aware authentication systems because they also require a large number of sensors capable of acquiring user location information. Although some of biometric collection equipment (e.g. cameras to obtain a face snapshot) may be relatively cheap, it is not always possible to install them inconspicuously, thus compromising their physical security.

Many biometric identification systems are relatively computationally expensive (e.g. face recognition); this may require transmitting the obtained biometric sample from the sensor where it was acquired to a centralized authentication server for evaluation. A large number of sensors would entail a complex communication infrastructure, which may or may not be combined with other communication facilities. Regardless of the implementation specifics, using an extensive communication infrastructure to transmit biometric samples for evaluation could further compromise the security of the system. An attacker may be able to intercept and modify the samples or bypass the sensors and feed previously recorded samples into the evaluation system.

VI. ISSUES OF PRIVACY

Here we refer to information privacy, which is generally concerned with the collection and handling of personal data. In particular, information privacy can be defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [24]. Location privacy is a special kind of information privacy concerning the control over the information about the person's location [11]. In particular, the users may be concerned when their location is revealed (they may be more concerned about revealing their current rather than past location), how (they may agree to tell their friends about their whereabouts, but would prefer not to automatically broadcast their daily activities) and to what extent (they may prefer to release their general location, e.g. a city or neighborhood, rather than precise coordinates) [13].

Location-aware applications offer the capability for automatic and real-time sensing of the user's location. The issue of location privacy is central to many of these applications because of the tension between the features enabled by location-awareness and the user's desire for control over their location information [3].

An excellent review of current research literature on location privacy could be found in [13]. According to many

user surveys, people seem to be unconcerned about location privacy in general. However, they usually become more sensitive when they realize how this data can be used, and what new information could be inferred from their location history (e.g. their true identity or addresses of their residences). Current research has demonstrated many feasible privacy attacks on anonymized location data; at the same time, many schemes to protect from such attacks have been proposed and tested.

A location-aware continuous authentication system deployed at an enterprise is very likely to generate a substantial stream of data that documents many aspects of user activity. Data collection and retention policies must be in place to control what elements of this data stream should be kept, for how long, and for what purpose. In the most realistic scenario, such records could be kept for auditing purposes in order to confirm any suspected security breaches or to analyze these records for potential red flags in the user behavior patterns or to detect any unusual activity. A conservative option to keep all collected records will quickly make any audits impossible due to the sheer volume of data. Although the final decision will remain with the enterprise where such a system is deployed, the exiting research is insufficient and lacks clear answers regarding what records should be stored, for how long, whether it should be aligned with other existing databases at the enterprise, and who should have access to such records [6,14].

VII. SUMMARY

Location-aware and continuous authentication systems at the workplace are shifting the balance between physical and information security, convenience and personal privacy. While biometric approaches seem to be the best fit for stand-alone continuous authentication, they do not appear to be the best choice for location-aware authentication systems due to their complexity, costs, and lack of portability. On the other hand, possession-based authentication systems (e.g. using RFID) may offer a cost-effective solution with a good balance between usability and the degree of security such a system provides.

Broad use of location-aware continuous authentication systems may raise a question whether their advantages are worth the intrusion into personal privacy. What data is being collected about the users? Is this data used only for the intended purposes? In order to answer these questions, one must often choose between moral values, such as privacy, and business values, such as security of intellectual of physical property, productivity, and profitability.

REFERENCES

[1] A. Azzini, S. Marrara, R. Sassi, and F. Scotti, "A fuzzy approach to multimodal biometric continuous authentication," Fuzzy Optimization And Decision Making, 7(3):243-256, 2008.

[2] J.E. Bardram, R.E. Kjær and M.Ø. Pedersen. "Context-aware user authentication – supporting proximity-based login in pervasive computing," Proc. 5th International Conference on Ubiquitous Computing, LNCS, 2864/2003:107-123, 2003.

[3] A.R. Beresford and F. Stajano, "Location privacy in pervasive computing," IEEE Pervasive Computing, 2(1):46-55, 2003.

[4] E. Bertino and M. Kirkpatrick, "Location-aware authentication and access control," Proc. International Conference on Advanced Information Networking and Applications, pp. 10-15, 2009.

[5] I. Brosso, A. La Neve, G. Bressan, and W.V. Ruggiero, "A Continuous authentication system based on user behavior analysis," Proc. 2010 International Conference on Availability, Reliability and Security, pp. 380-385, 2010.

[6] T.G. Calderon, A. Chandra, and J.J. Cheh, "Modeling an intelligent continuous authentication system to protect financial information resources," International Journal of Accounting Information Systems, 7(2):91-109, 2006.

[7] C.M. Carrillo. "Continuous authentication for authorized aircraft personnel: a proposed design," Masters' Thesis, Naval Postgraduate School, Monterey, CA, Department of Computer Science, 2003.

[8] M.L. Damiani, E. Bertino, B. Catania, and P. Perlasca, "GEO-RBAC: a spatially aware RBAC," ACM Transactions on Information and System Security, 10(1), 2007.

[9] I.G. Damousis, D. Tzovaras, and E. Bekiaris, "Unobtrusive multimodal biometric authentication: the HUMABIO project concept," EURASIP J. Adv. Signal Process, 2008.

[10] D.E. Denning and P.F MacDoran, "Location-based authentication: grounding cyberspace for better security," Computer Fraud & Security, 1996(2):12-16, 1996.

[11] M. Duckham and L. Kulik, "Location Privacy and location-aware computing," in Dynamic & Mobile GIS: Investigating Change in Space and Time, J. Drummond, et al., Eds., CRC Press, Boca Raton, FL, 2006.

[12] S. Furnell and K. Evangelatos, "Public awareness and perceptions of biometrics," Computer Fraud & Security, 2007(1):8-13, 2007.

[13] J. Krumm, "A survey of computational location privacy," Personal Ubiquitous Computing, 13(6):391-399, 2009.

[14] S. Kurkovsky, E. Syta, and B. Casano, "Continuous RFID-enabled authentication and its privacy implications," Proc. IEEE International Symposium on Technology and Society, pp. 103-110, 2010.

[15] V. Lee, "Biometrics and identity fraud," Biometric Technology Today, 16(2) 7-11, 2008.

[16] K. Niinuma, U. Park, and A.K. Jain, "Soft biometric traits for continuous user suthentication," To appear in IEEE Transactions On Information Forensics and Security, 2010.

[17] M. Orozco, Y. Asfaw, S. Shirmohammadi, A. Adler, and A. El Saddik, "Haptic-based biometrics: a feasibility study," Proc. 14th Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems, pp, 265-271, 2006.

[18] T. Parker, "Are we protected? The adequacy of existing legal frameworks for protecting privacy in the biometric age," Proc. 3rd International Conference on Ethics and Biometrics, LNCS, 6005/2010: 40-46, 2010.

[19] I. Ray, M. Kumar, and L. Yu, "LRBAC: a location-aware role-based access control model," Information Systems Security, LNCS, 4332/2006:147-161, 2006.

[20] F. Sabena, A. Dehghantanha, and A.P. Seddon, "A review of vulnerabilities in identity management using biometrics," Proc. 2nd International Conference on Future Networks, pp. 42-49, 2010.

[21] R.S. Sandhu, E.J. Coyne, H.L Feinstein, and C.E Youman, "Role-based access control models," Computer , 29(2):38-47, 1996.

[22] A. Seleznyov and S. Puuronen, "Using continuous user authentication to detect masqueraders," Information Management & Computer Security, 11(3): 139-145, 2003.

[23] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics," IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4):687-700, 2007.

[24] A.F. Westin, Privacy and freedom. Atheneum, New York, 1967.