Chapter 42
Biometric Authentication Techniques in Online Learning Environments

Jack Curran
Open University, UK

Kevin Curran
Ulster University, UK

ABSTRACT

The deployment of online e-learning can lead to many security risks, such as confidentiality loss, exposure of critical data, availability and destruction of publicly available information services. Security and proper authentication is critical in any online learning environment because any flaws can affect perceptions of its trustworthiness. Biometric authentication is increasingly being used in the newer generation of online learning environments for authentication of remote learners. Biometrics scan unique physiological characteristics in humans to identify people. These include fingerprints, iris, retina, voice, face, gait, and odor. The authors look at the state of biometric authentication techniques applicable to online learning environments and provide a more in-depth examination of face- and iris-based authentication systems for proper identification of learners.

BACKGROUND

There is becoming close to 100% adoption of e-learning environments in education institutions. Online learning environments are by their nature subject to all the attacks that online systems are vulnerable to (Adams & Blandford, 2003). Their 'low risk' nature on roll-out however leave many of the online learning environment content management more open than usual (Chen and He, 2013). Educational institutions tend to underestimate their attack surface and implications of being penetrated (Zuev, 2012). There is also the added weakness of Denial of service attacks which render e-learning environments unavailable to students. Commons risks however are unauthorized modification or deletion of educational materials,

DOI: 10.4018/978-1-7998-8047-9.ch042

and the equally dangerous problem unique to remote e-learning models of identity theft, impersonation, and weak authentication (Ayodele et al., 2011). The roll-out of online e-learning can lead to many security risks, such as loss of confidentiality, the exposure of critical data, availability and destruction of publicly available information services (Srivastava & Sinha, 2013). Security & proper authentication is critical as a means to retain user trust in any online learning environment because any risk can affect perceptions of its trustworthiness (Weippl & Ebner, 2008). Therefore, it is crucial to try to identify any underlying factors that lead to security issues in online learning and identify the limitations of security in place (Yao et al., 2011). The next step of course is to develop mitigations for any weaknesses uncovered.

Authentication is a key aspect for online learning (Raitman et al., 2005). There are several ways to achieve this. They can use knowledge-based authentication where users enter passwords or pins. They can use token-based authentication with key card, smart-phones or some security token or they can use biometric based authentication such as fingerprints, palm print, a retinal scan, or a face scan (Alotaibi & Argles, 2011; Garfinkel & Spafford, 1996). Among these authentication methods, user logins are the simplest means for providing identity and access services while retinal or face scans are the more difficult - but seen as the stronger (Song et al., 2013). In fact, biometric authentication seems to be increasingly used in the newer generation of online learning environments for authentication (Wang et al., 2013).

Humans possess many unique physiological body and shape characteristics that distinguish one from another. Some of these biometric characteristics in humans include fingerprints, iris, retina, voice, face, Palm prints and palm veins (Li & Kot, 2013). Some are more unique and secure than others. The uniqueness of a biometric feature that nearly every human possesses is determined by how many possible combinations can exist. Such a measure maximizes between-person random variations while at the same time minimizes within-person variability (Teoh et al., 2004). A biometric with many combinatorial possibilities means the possibility of two individuals in possession of identical patterns becomes increasingly less probable, therefore making it more secure as a biometric authenticator. There are two categories of biometrics. One deals with the physiological aspect, such as patterns, prints and physical features and the other is behavioural concentrating on aspects such as typing patterns, walking gaits, mannerisms, voice and computer usage patterns (Ratha & Zhang, 2010). An example of an insecure biometric authenticator would be the colour of people's eyes. If someone had brown eyes and they were enrolled on a database, everyone else with brown eyes who were to attempt to enrol themselves would be authenticated as being the first individual which was scanned originally (Pfleeger & Pfleeger, 2007). Therefore, this is insecure as anyone with brown eyes can be an imposter to the original individual who was enrolled. If, however there was a biometric feature with the probability of having the same pattern with another human being 1/1,000,000,000, then this would be considered secure as it is almost impossible to have two individuals with the same biometric pattern.

Biometric scans can be passive or contact. Passive scanning means no physical contact is required e.g. in iris scanning, where a user is told to stand a certain distance from the camera. Contact biometrics is when contact with a physical object is needed e.g. finger print scanning, when a user is asked to place their specified finger upon a scanning surface (Farooq et al., 2007). Compared with traditional password or token-based authentication, biometrics are considered more secure when executed correctly. Password and token-based methods can only authenticate a person possesses a token or knows a password. However, biometrics can check that a person is who they claim to be. Deployment of proper biometric solutions should significantly reduce identity thefts with great benefits for the economy by eliminating passwords from the equation in place of more reliable solutions. Trust is particularly important for financial institutions and merchants as well as consumers (identify theft, account blocking inconvenience) alike so we

can expect the first to deploy biometrics in large scale will be those involved in mobile payments and other financial organisations.

There are of course many biometric solutions. None are a silver bullet and one size does not fit all. The accuracy of facial recognition systems varies greatly due to factors such as lighting, angle & camera sensitivity and more. Facial techniques can also be thrown off by facial characteristics or a person simply wearing glasses will be different with sunglasses, no glasses and colour of the ambient light. Fingerprint readers likewise are affected by temperature and other factors. Fingerprint scanners in phones are deployed en mass now due to Apples Touch ID system. They have of course been on laptops for years but hardly used. The Touch ID system from Apple is quite impressive from a security perspective. Fingerprint scanners are not the solution however as we simply leave fingerprints on every surface we touch. There have been many examples of Apples' Touch ID been bypassed using scanners, latex and patience. This chapter provides an overview of popular biometric authentication approaches and provides a more in-depth examination of face and iris-based authentication systems

AUTHENTICATION

The alphanumeric password is revealing itself as unfit for purpose. As the number of devices (approaching 20 billion) and services which need access control increases, this legacy standard has reached a tipping point when measured by the vast number of identity thefts and account hijacks impacting people in recent times. There are more secure, less costly and more adoptable alternatives to the password/PINs approach. It is estimated that online "direct" fraud is costing the global economy around £60bn a year. The associated indirect costs of identity theft and recovery have not been fully quantified but is possibly many times the actual direct costs (Rane, 2014). Large e-commerce merchants believe that fraud is inevitable but understand that their prevention efforts will result in more positive customer relationships. The current most widespread authentication approach employs passwords. Passwords are weak and susceptible to many types of attacks as the security is dependent on a users' ability to keep the password secret from eavesdropping in its many forms. If we were to invent it today, we might find that it does not pass quality control for making financial transactions remotely, such as fund transfers and other payments through an Internet banking channel. There is also the question of the cost of support associated with user ID and password complexity as IT support staff often need to spend extra time dealing with authentication problems, such as helping staff reset passwords that are locked after a certain number of failed entry attempts (Dunker, 2003).

There are other clever biometric systems on the market using contextual information (location etc) in clever ways (Dunker, 2003). For instance, many are not yet familiar with keystroke dynamics. Keystroke dynamics is where keystroke logging can be analyzed. The time to get to and depress a key (seek-time), and the time the key is held-down (hold-time) can be very specific to a person, regardless of how fast they are going overall. Most people have specific letters that take them longer to find or get to than their average seek-time over all letters, but which letters those are may vary dramatically but consistently for different people. Right-handed people may be statistically faster in getting to keys they hit with their right-hand fingers than they are with their left-hand fingers. Index fingers may be characteristically faster than other fingers to a degree that is consistent for a person day-to-day regardless of their overall speed that day. Normally, all that is retained when logging a typing session is the sequence of characters corresponding to the order in which keys were pressed and timing information is discarded. Keystroke

dynamic information which is normally discarded, can be used to verify or even try to determine the identity of the person who is producing those keystrokes. There are several home software and commercial software products which claim to use keystroke dynamics to authenticate a user such as BioTracker, ID Control, TypeWATCH, Authenware, Probayes and KeyTrac.

There is also voice as a biometric technique. Voice however has to be measured against both the ambient background e.g. a restaurant, a train, corner shop street or sports arena (Masala et al., 2017). Again, fingerprints taken when the finger is flat will be different when misaligned, wet, dirty or practically frozen. There really has not been much movement in trying to implement voice authentication. It does play a part in some multi factor systems. The main barrier to any widespread adoption has been the problem of aural eavesdropping. Quite simply, casual or malicious bystanders may overhear private information spoken by screen readers or users (Rane, 2014). There are some niche areas where it is adopted. Take for instance the special needs of disabled citizens. In the context of disability, the process of authentication is stressful for many users looking to access devices or services. For example, individuals who are blind have difficulties with processes of authentication such as Captcha which cut them off from bank accounts and all other online access points because they must visualise and input meaningless character sequences. The spoken option is not good. Voice authentication can play an important role here (Patel et al., 2015).

These sources of potential error create two measuring levels that biometrics algorithms build in to their calculations which are false acceptance and false rejection. If this is not managed and measured properly, it can lead to a bad user experience which has been a problem with commercialisation of such technologies in the past decade as they seek to achieve the elusive 100% accuracy rate. The objective of biometric identity authentication is to establish a bond of trust between an organization and the user who is requesting system access. More specifically, identity authentication ascertains a level of trust regarding who the user claims to be (Patel et al., 2015). It follows that the more accurate any chosen authentication method the user can present to prove his/her identity, then the stronger this bond of trust becomes. It is feasible that biometric authentication becomes the de facto form of providing credentials (although it should be combined with multi-factor methods). Hardware devices do potentially offer ideal security but often the problem is the need to carry such a device on the person (Rane, 2014). Hence the move towards making our mobile phones the de facto hardware device. One popular hardware approach for authentication is smart cards. Smart cards technology provides an excellent medium for storing biometrics. A smart card can provide a strong authentication platform in our pocket. Mobile phones and smart cards can be used for both physical and logical access authentication (Sutcu et al., 2007).

There are problems in general with hardware security tokens. Firstly, they involve additional costs, such as the cost of the token and any replacement fees. Users always need to carry the token with them. Users need multiple tokens for multiple Web sites and devices (Daugman, 2006). Finally, they do not protect fully from man-in-the-middle attacks (i.e., attacks where an intruder intercepts a user's session and steals the user's credentials by acting as a proxy between the user and the authentication device without the user's knowledge). Basically, if you lose the token, you lose control. A related area is Digital Certs on USBs or Smart Cards. Here however are problems as well as they require users to carry an additional smart card reading device or USB. They also involve additional cost, such as certifying authority's subscription cost. You need multiple certificates for different sites or devices. It can be difficult for non-authorized users to extract the private key when stored on a smart card and they require user training for certificate generation and use (Merhav, 2017).

One technique which should be combined with any biometric authentication is multi-factor authentication. Multifactor authentication reduces authentication risk by involving separate types of factors that would require an attacker to use different methods of attack, thus making a breach more difficult. Multi-factor authentication combines at least two of the following methods to strongly authenticate a user. These are something you know (typically a password/PIN), something you have (a trusted device identifier that is not easily duplicated) and something you are (your unique biometrics). In order to qualify as multi-factor authentication, two items must be combined from different categories, therefore a PIN plus a password is not actually multi-factor, since both of these are something you know. Full three factor authentication when combined with a device ID allows you to easily combine "what we have" and "what we know" with the important "who we are". This is important for future security systems.

What however is now considered best practice is to use tools like tools like Google Authenticator or an RSA token which can also prove possession. These do not involve a communication which can be as easily eavesdropped upon nor a sim-card that can be replaced. In fairness however, the 2-factor attacks just described do involve targeting an individual and some high level of skill in addition to hardware. The problem is that attacks never get worse and there is always someone out there making the hardware cheaper and the software easier to use so we can expect to see lesser skilled attackers exploiting weaknesses in multi-factor authentication - which for a brief period did what it said on the box.

Biometric solutions may provide us with the solution we need to more fully secure our online learning environments. They are playing an increasingly significant role in new online learning environments (Ayodele et al., 2011; Chen and He, 2013). Next, we examine face and iris-based authentication systems.

BIOMETRIC AUTHENTICATION SYSTEMS

The process of face scanning pertains to the ability of measuring the distance between key features and points of the face known as references. Key reference features on the face include distance between irises, length of eye brows, length of philtrum, width of nose, height and shape of eye lids and distance from eyes to mouth (Li & Kot, 2013). When scanning a detainee's face, all references on the face are combined into a biometric facial template which is enrolled in a database. This template is compared to all pre-existing facial templates and if a pre-defined threshold of measurement values is matched with a template stored on the database, then the detainee is identified as being the same person. Occasionally there may be false matches, meaning it is not the same person even though their measurements exceeded the threshold.

Several hundred million persons around the world have been enrolled in iris recognition systems for purposes such as passport-free automated border-crossings and national ID programs (BBC, 2012). A key advantage of iris recognition, in addition to its speed of matching and extreme resistance to false matches, is the stability of the iris as an internal and protected, yet externally visible organ of the eye. The process of iris scanning involves measuring the various minutiae of the iris. There are 250 points within the iris, of which can take on one shape from a plethora of varying types of shapes creating an almost unique iris pattern due to the sheer amount of combinatorial possibilities. When all minutiae of the iris are scanned and recognised, it forms a biometric template. This is stored for checking against future scans to look for a match (Daugman, n.d).

Convenience

Facial scanning may be inconvenient to detainees as they will have to remove any facial obstructions in order to scan the face such as glasses, contact lenses, hats, makeup, fake eyelashes or fake tan. New developments in facial recognition technology allow for 3D capture of a subject's face. It enables greater precision and allows for a much wider range of angles as opposed to flat RGB. Additionally, new research has seen the introduction of technology that allows for subjects to have varying facial expressions and to still be recognised as the same person previously captured in a different expression (Chen et al., 2014). Facial scanning is convenient as detainees simply have to be facing in the general direction of the scanner. This also allows increased accessibility to vision impaired individuals who may not be able to precisely orientate their face to look in a specific direction.

Iris scanning requires users to face the scanner. Their face must retain a neutral expression, otherwise the iris could be obstructed by the eyelids. Iris recognition works with clear contact lenses, eyeglasses, and non-mirrored sunglasses. Deviations in position or rotation of a subject's face are also not allowed as they can result in a failed scanned (Daugman, n.d).

Reliability

A major point to consider when comparing iris vs facial biometrics is identity theft. It is possible to have a facial biometric stolen and used against a biometric facial scanning system to trick it. An image or scan of a victim's face can be stolen from afar without the victim ever knowing. A scanner can however use thermal imaging to detect whether the facial substitution is living or not so as to render paper-based images useless (Cai et al., 2018). If a migrant were to have altered their facial appearance, a facial recognition machine may not be able to recognise them. This can be due to many reasons such as facial hair growth or removal, hairstyle change, facial injury or face altering surgery. This could mean needing to rescan detainees.

Iris scanning does not have this problem as the iris, unless permanently damaged will remain the same since the initial scan (Bleicher,2005). This can be as long as decades. Facial scanning is not as effective as other biometrics in identifying minorities when most of the subjects used in training the technology were from the majority group (Bonsor & Johnson, 2016). Iris scanning in such cases would fare better as there are a significantly lower amount of non-iris scannable minorities.

Acceptability

There may be use cases where individuals may not want to have their biometric identity stored digitally on a database. They may desire to retain their privacy. If data from a biometric database is leaked, that data may be used in identity theft (Mordini & Tzovaras, 2012). This is a key issue with regards biometrics due to the irrevocable link between biometric traits and a persistent information record concerning an individual. Unlike most other forms of recognition, biometric techniques are firmly tied to a physical body and this link between personal records and biometrics can have negative consequences for individuals (Pato & Millett, 2010). The problem of course with losing biometric data belonging to people is that they cannot get it back or change it so if you lose the data for someone's fingerprints - it is out there, and they have no way of course to change their fingerprint pattern.

An advantage of iris scanning is that it is akin to taking a photograph and can be done from 10 cm to a few meters distance. The person being identified does not have to touch any equipment that has recently been touched by a stranger. This is important for acceptability as it eliminates an objection that has been raised in some cultures against fingerprint scanners, where a finger needs to touch a surface, or retinal scanning, where the eye must be brought very close to an eyepiece (Martin, 2011).

FACE AND IRIS-BASED AUTHENTICATION CAPTURE

Iris

Iris scanning utilises infrared lights for scanning as well as the addition of digital camera technology to capture a complex and detailed iris (Barra et al., 2015). When an iris has light shone upon it, the eye will compensate for the exposure and dilate. However, inanimate objects will not be able to perform this function, or at the realism level needed to be considered an actual iris by the scanner Therefore, if someone attempts bypassing the iris scanner, they may be able to get past the first stage of recognising the iris pattern, but they will most likely fail upon the second test for life in the iris. Initially the scanner must localize the inner and outer boundaries of the iris. Subsequent subroutines detect and exclude eyelids, eyelashes, and any specular reflections that often occlude parts of the iris. The pixel set containing the iris is normalized by a rubber-sheet model to compensate for pupil dilation or constriction. This is next analyzed to extract a bit pattern encoding the information needed to compare two iris images (Daugman, 2006).

Face

Capturing an individual's face for biometric facial recognition is not as complex as iris scanning. Facial scanning can even be performed from simple 2D photographs. In most high end facial scanning systems, various hardware exists to ensure the security of the scan and to avoid circumvention using substitute fake faces (Kisku, 2016). Some items that may exist in a biometric facial scanner are a 2D camera system, infrared dot projector and thermal imaging camera. During a facial scan, various checks and processes will occur such as extracting colour information and texture detail. A dot projector will also be used to capture 3D facial features to ensure the subject is not a flat high resolution 2D image. A thermal heat map can also be used to detect if the object is living.

FACE AND IRIS-BASED AUTHENTICATION PROCESSING

Iris

Once the user's facial biometric template has been captured, an iris template is generated. This template encodes the pattern of the iris which can later be compared against all pre-existing iris template stored within the database to authenticate or identify individuals (Sutcu et al., 2007). Unlike current facial processing techniques, iris processing is remarkably fast, testing has revealed iris match comparisons on large databases are completed with millions per second on only 1 CPU core (Patel et al., 2015). Ac-

curacy and false match rates are not sacrificed either. False match rates have been reported to be very low. Thus, with the speed of iris template processing, no other methods are required for speeding up the process (Rane, 2014).

Face

Once the user's facial biometric template has been captured, it must be compared against pre-existing templates to identify the individual. Some databases contain millions of unique facial templates (Weaver, 2006). This can take a long time therefore leading to slow authentication of users (Ratha et al., 2001). A solution involves categorising parts of each user's template face at the time of creation. This effectively divides templates into categories based on their facial features and what category each part slots into such as eye colour, ear shape, skin colour, eye shape, lip shape, gender, nose shape, face height and jaw line. Each of these individual categories when viewed individually have few user templates however, as a collective there could be millions of templates (Open University, 2018). Eventually there will be a point reached where the number of templates left to be processed based on the final category is satisfactorily low to individually processing of the remaining templates that fit within the category. This division method speeds processing time up significantly (Merhav, 2018).

FUTURE RESEARCH DIRECTIONS

Biometrics will play a role in authentication in many online learning environments in the future as biometrics-based authentication provides a real-world alternative to using passwords and pins. Biometrics can play a role in most areas where authentication of a service is necessary. It works in validating the identity of users by measuring unique physiological and behavioural characteristics of individuals. Such a measure maximizes between-person random variations while at the same time minimizes within-person variability. In contrast with passwords and pins, a biometric identifier cannot be lost, forgotten or shared. One can choose from a large list that includes finger, face, retinal scan, iris, gait, vein infrared thermogram, hand geometry and palm print or from a combination of all these identifiers termed multimodal-biometrics.

There are also moves to utilise novel biometric systems such as the Tongue. The tongue is a unique vital organ which is pretty well protected inside the mouth. Hence it is affected by external factors. The Dorsum of the tongue shows a lot of information along with its visual differences in shape, texture and pattern which is known as the tongue print. The tongue therefore exhibits rich textural patterns. (Trivandrum et al., 2018) demonstrate a Local Binary Pattern (LBP) algorithm for extracting features which are then trained by a linear Support Vector Machine (SVM) for personal identification. From a database of 136 tongue print images of 34 individuals, they achieved an accuracy of 97.05% for identification. This was one of the earliest studies where texture patterns are extracted from tongue images for biometric authentication. We can expect to see more work in this interesting area.

The biggest change in future learners using online learning environments might be the rise of the mobile device as the device of choice for biometric reading. We now see that mobile devices are increasingly the mainstay of a person's online activities. Most of the market dominating smartphones now have biometric readers or sensors already incorporated into the hardware. Biometrics will also have some impact on the home with regards the need for additional hardware costs such as scanners. There are

also extra costs needed for deployment, support and maintenance. It may also not be suitable for mass-consumer deployment just yet. The main place that biometrics play a role in the home is in door entry systems. Of late there have been a few breakthroughs in biometric technology that can help make these systems even more secure. Japan's Fujitsu has miniaturised iris recognition technology which takes barely a second, meaning the home can be unlocked with just a look, and the camera can be placed at normal viewing distance, not the 10cm required by most iris scanners.

While codes and fingerprints work well, this technology means gloves can be kept on in cold weather and firing up the phone with one hand is that little bit easier. The phone itself will be able to register its owner's iris pattern for the first time, a process which takes 10 seconds, using an LED light that shines into the eye and a small infrared camera. Fujitsu hopes to persuade manufacturers, software and app developers to incorporate its invention for commercial release this year. Qualcomm have a technology called sense ID. It is a '3D' fingerprint scanner technology. It not only scans the print but also scans the depth of the ridges. You cannot therefore use a photo to bypass this authentication mechanism. This could be better than touch id. It can also scan through glass, sapphire, plastic.

Specifically, biometrics can be used by online learning environment system admins to grant users only select features in a system. Voice authentication has been trialled in some online systems case studies. However, there really has not been much movement in trying to implement voice authentication. It does play a part in some multi factor systems. The main barrier to any widespread adoption has been the problem of aural eavesdropping. Quite simply, casual or malicious bystanders may overhear private information spoken by screen readers or users. Others involved in the home automation voice command systems include GEO Semiconductor. They recently launched Granta smart home automation technology which contains voice and vision control capabilities designed for user interfaces for home security and entertainment control devices (Cericola, 2013). It was demonstrated at the 2015 Voice Biometrics Conference in San Francisco. Granta is primarily targeted at home security, smart TC and entertainment markets.

CONCLUSION

We provided here an overview of security in online learning environments which are by their nature subject to many of the attacks that standard online systems are vulnerable to also (Adams & Blandford, 2003). Their 'low risk' nature on roll-out however leave many of the online learning environment content management more open than usual (Chen and He, 2013). Educational institutions tend to underestimate their attack surface and implications of being penetrated (Zuev, 2012). There is also the added weakness of Denial of service attacks which render e-learning environments unavailable to students. Commons risks however are unauthorized modification or deletion of educational materials, and the equally dangerous problem unique to remote e-learning models of identity theft, impersonation, and weak authentication (Ayodele et al., 2011). Biometric authentication is increasingly being used in the newer generation of online learning environments for authentication.

We also looked at biometrics based authentication for online learning environments and in particular Face and iris-based authentication capture & processing procedures. We highlighted the actual scientific methods by which an Iris and a Face are scanned to capture the unique physiological details which comprise each. The discussion on the processing firstly focussed on the Iris technique where a biometric template is generated and the accuracy & speed of iris scanners. In discussing facial process-

ing, we highlighted the need to overcome slow authentication of users in large databases through the categorisation of features such as eye colour, ear shape, skin colour, eye shape, lip shape, gender, nose shape to speeds up processing time significantly. Some religions that choose to wear a burka may not wish to unveil their face in public to a facial scanner. However, iris scanning enables these people to be biometrically identified as their eyes are still visible through a burka.

Facial injuries might affect the ability to facially recognise an individual as their face may have been altered. If the individual's iris has not been damaged, a facial injury will not be an issue. Iris recognition is also more secure. The commercially deployed iris-recognition algorithm '*IrisCode'*, has an unprecedented false match rate better than 10^{-11}. The Hamming distance threshold of 0.26 used, means that up to 26% of the bits in two IrisCodes can disagree due to imaging noise (Daugman, 2006). While there are some medical and surgical procedures that can affect the colour and overall shape of the iris, the fine texture remains remarkably stable over many decades. Some iris identifications have succeeded over a period of about 30 years. Identical twins can also be uniquely identified due to different iris patterns. Identical twins are problematic for facial scanners. Iris recognition is significantly more difficult to circumvent due to the complexity within the iris. Iris recognition removes the need for physical contact with the biometric recording device, but it does require a clear line of sight of the detainee's iris (Dunker, 2003). It must be noted however that like other photographic biometric technologies, iris recognition is susceptible to poor image resolution, with related failure to enrol rates (BBC, 2012).

Biometrics based authentication do provide a robust alternative to using passwords and pins. It validates identity of users by measuring unique physiological and behavioural characteristics of individuals. Such a measure maximizes between-person random variations while at the same time minimizes within-person variability. In contrast with passwords and pins, a biometric identifier cannot be lost, forgotten or shared. One can choose from a large list that includes finger, face, retinal scan, iris, gait, vein infrared thermogram, hand geometry and palm print or from a combination of all these identifiers termed multimodal-biometrics. The biggest change in the future might be the rise of the mobile device as the device of choice for biometric reading. We now see that mobile devices are increasingly the mainstay of a person's online activities. Most of the market dominating smartphones now have biometric readers or sensors already incorporated into the hardware. Biometrics will also have some impact on the workplace with regards the need for additional hardware costs such as scanners. There are also extra costs needed for deployment, support and maintenance. It may also not be suitable for mass-consumer deployment.

While biometrics are promising, the true 'strong' solution might simply be multifactor authentication. Multifactor authentication reduces authentication risk by involving separate types of factors that would require an attacker to use different methods of attack, thus making a breach more difficult. Multi-factor authentication combines at least two of the following methods to strongly authenticate a user (1) Something you know (typically a password/PIN) (2) Something you have (a trusted device identifier that is not easily duplicated) and (3) Something you are (your unique biometrics). To qualify as multi-factor authentication, two items must be combined from different categories, therefore a PIN plus a password is not actually multi-factor, since both items are something you know. Full three factor authentication when combined with a device ID allows enterprises to easily combine "what we have" and "what we know" with the all-important "who we are", thereby integrating a core benefit to future home automation security systems. Security & proper authentication is critical as a means to retain user trust in any online learning environment because any risk can affect perceptions of its trustworthiness and biometrics properly implemented may be a good fit.

REFERENCES

Adams, A., & Blandford, A. (2003). Security and online learning: To protect or prohibit. *Usability Evaluation of Online Learning Programs*, 331-359.

Alotaibi, S. J., & Argles, D. (2011). FingerID: A new security model based on fingerprint recognition for personal learning environments (PLEs). In *Global Engineering Education Conference (EDUCON)* (pp. 142-151). IEEE 10.1109/EDUCON.2011.5773128

Ayodele, T., Shoniregun, C. A., & Akmayeva, G. (2011). Towards e-learning security: A machine learning approach. In *Information Society (i-Society), 2011 International Conference* (pp. 490-492). IEEE.

Barra, S., Casanova, A., Narducci, F., & Ricciardi, S. (2015). Ubiquitous iris recognition by means of mobile devices. *Pattern Recognition Letters, 57*, 66-73. doi:10.1016/j.patrec.2014.10.011

BBC. (2012). Black Hat: Iris scanners 'can be tricked' by hackers. *BBC Technology*. Available at: http://www.bbc.co.uk/news/technology-18997580

Bleicher, P. (2005). Biometrics comes of age: despite accuracy and security concerns, biometrics are gaining in popularity. *Applied Clinical Trials*. Available at: http://www.appliedclinicaltrialsonline.com/biometrics-comes-age

Bonsor, K., & Johnson, R. (2016). How Facial Recognition Systems Work. *HowStuffWorks*. Available at: https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm

Cai, Y., Jiang, H., Chen, D., & Huang, M. (2018). Online learning classifier based behavioral biometric authentication. *2018 IEEE 15th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, 62-65. doi: 10.1109/BSN.2018.8329659

Cericola, R. (2013). Granta Will Bring Voice Control to Home Automation. *Electronic House*. Available at: https://www.electronichouse.com/smart-home/geo-semiconductor-speechfx-and-voicevault-partner-up-for-granta

Chen, S., Pande, A., & Mohapatra, P. (2014). Sensor-assisted facial recognition: an enhanced biometric authentication system for smartphones. *Proceedings of the 12th annual international conference on Mobile systems, applications, and services (MobiSys '14)*, 109-122. 10.1145/2594368.2594373

Chen, Y., & He, W. (2013). Security Risks and Protection in Online Learning: A Survey. *The International Review of Research in Open and Distance Learning*. Available at: http://www.irrodl.org/index.php/irrodl/article/view/1632/2712

Daugman, J. (2006). Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons. *Proceedings of the IEEE*, *94*(11), 1927–1935. doi:10.1109/JPROC.2006.884092

Daugman, J. (n.d.). Iris recognition. *International Center for Disability Resources on the Internet*. Available at http://www.icdri.org/ biometrics/ iris_biometrics.htm

Davida, G., Frankel, Y., & Matt, B. (1998). On enabling secure applications through off-line biometric identification. *IEEE Symp. Security and Privacy*, 148-157. 10.1109/SECPRI.1998.674831

Dunker, M. (2003). Don't Blink: Iris Recognition for Biometric Identification. *SANS Institute InfoSec Reading Room*. Available at http://www.sans.org/ reading_room/ whitepapers/ authentication/dont-blink-iris-recognition-biometric-identification_1341

Farooq, F., Bolle, R., Jea, T., & Ratha, N. (2007). Anonymous and revocable fingerprint recognition. *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, 1-7. DOI: 10.1109/CVPR.2007.383382

Garfinkel, S., & Spafford, G. (1996). Practical Unix and Internet security. In *INET 96*. O'Reilly & Associates, Inc.

Kisku, D., Gupta, P., & Sing, J. K. (2016). *Advances in Biometrics for Secure Human Authentication and Recognition*. London: CRC Press.

Li, S., & Kot, A. (2013). Fingerprint combination for privacy protection. *IEEE Transactions on Information Forensics and Security*, *8*(2), 350–360. doi:10.1109/TIFS.2012.2234740

Martin, Z. (2011). Biometric Trends: Will emerging modalities and mobile applications bring mass adoption? *SecureIDNews*. Available at: https://www.secureidnews.com/news-item/biometric-trends-will-emerging-modalities-and-mobile-applications-bring-mass-adoption/?tag=biometrics&tag=Law_Enforcement

Masala, G., Ruiu, P., & Grosso, E. (2017). *Biometric Authentication and Data Security in Cloud Computing*. Computer and Network Security Essentials.

Merhav, N. (2017). The generalized stochastic likelihood decoder: Random coding and expurgated bounds. *IEEE Transactions on Information Theory*, *63*(8), 5039–5051. doi:10.1109/TIT.2017.2689787

Merhav, N. (2018). Ensemble Performance of Biometric Authentication Systems Based on Secret Key Generation. *2018 IEEE International Symposium on Information Theory (ISIT)*, 1455-1459. 10.1109/ISIT.2018.8437768

Mordini, E., & Tzovaras, D. (2012). *Second Generation Biometrics: the Ethical and Social Context*. Springer-Verlag.

Open University. (2018). *T215 Communication and information technologies Module Handbook*. Open University; doi:10.1007/978-94-007-3892-8

Patel, V., Ratha, N., & Chellappa, R. (2015). Cancelable Biometrics: A review. *IEEE Signal Processing Magazine*, *32*(5), 54–65. doi:10.1109/MSP.2015.2434151

Pato, J., & Millett, L. (2010). *Biometric Recognition: Challenges and opportunities*. National Academies Press.

Pfleeger, C., & Pfleeger, S. (2007). *Security in Computing* (4th ed.). Boston: Pearson Education.

Raitman, R., Ngo, L., Augar, N., & Zhou, W. (2005). Security in the online e-learning environment. In *Advanced Learning Technologies, 2005. ICALT 2005. FIFTH IEEE International Conference* (pp. 702-706). IEEE.

Rane, S. (2014). Standardization of biometric template protection. *IEEE MultiMedia*, *21*(4), 94–99. doi:10.1109/MMUL.2014.65

Ratha, N., Connel, J., & Bolle, R. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, *40*(3), 614–634. doi:10.1147j.403.0614

Ratha, N., & Zhang, D. (2010). Privacy protection in high security biometrics applications. In A. Kumar & D. Zhang (Eds.), *Ethics and Policy of Biometrics* (pp. 62–69). Springer. doi:10.1007/978-3-642-12595-9_9

Song, K., Lee, S. M., & Nam, S. C. (2013). Combined biometrics for e-learning security. ISA 2-13. *ASTL*, *21*, 247–251.

Srivastava, A., & Sinha, S. (2013). Information security through e-learning using VTE. *International Journal of Electronics and Computer Science Engineering*, *2*(18), 528–531.

Sutcu, Y., Li, Q., & Memon, N. (2007). Protecting biometric templates with sketch: Theory and practice. *IEEE Transactions on Information Forensics and Security*, *2*(3), 503–512. doi:10.1109/TIFS.2007.902022

Teoh, A., Ling, D., & Goh, A. (2004). Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, *37*(11), 2245–2255. doi:10.1016/j.patcog.2004.04.011

Trivandrum, S., Shali, N., Zacharias, G., & Anna, P. (2018). Identification of tongue print images for forensic science and biometric authentication. *Journal of Intelligent & Fuzzy Systems*, *34*(3), 1421–1426. doi:10.3233/JIFS-169437

Wang, F., Ge, B., Zhang, L., Chen, Y., Xin, Y., & Li, X. (2013). A system framework of security management in enterprise systems. *Systems Research and Behavioral Science*, *30*(3), 287–299. doi:10.1002res.2184

Weaver, A. C. (2006). Biometric Authentication. *Computer*, *39*(2), 96–97. doi:10.1109/MC.2006.47

Weippl, E., & Ebner, M. (2008). Security privacy challenges in e-learning 2.0. In *World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education* (Vol. 2008, No. 1, pp. 4001-4007). Academic Press.

Yao, H., & Ji, Y. (2011). Security protection for online learning of music. In *Computer Communication and Networks (ICCCN), 2011 Proceedings of 20th International Conference* (pp. 1-4). IEEE. 10.1109/ICCCN.2011.6005740

Zuev, V. (2012). E-learning security models. *Management*, *7*(2), 24–28.

This research was previously published in Biometric Authentication in Online Learning Environments; pages 266-278, copyright year 2019 by Information Science Reference (an imprint of IGI Global).