ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 6, 225-235 (2017)

www.astesj.com

Special issue on Advancement in Engineering Technology

ASTESJ

ISSN: 2415-6698

A Taxonomy for Enhancing Usability, Flexibility, and Security of User Authentication

Susan Gottschlich*

Raytheon Co., 1001 Boston Post Road East, Marlborough, MA, 01752, 508-490-2339

ARTICLE INFO

Article history:
Received: 29 August, 2017
Accepted: 03 December, 2017
Online: 15 December, 2017

Keywords:
Continuous authentication
Multifactor authentication
Internet of Things
Software Defined
Wearable devices
Cybersecurity
Biometrics

ABSTRACT

Two technology trends - a move toward software defined capabilities and toward networked devices – support both unprecedented innovations and requirements for security. A fundamental aspect of security is user authentication, which allows devices and software applications to establish their user's identity and identity is in turn used to establish which of its capabilities the user is authorized to access. While multiple authentication steps, known as multifactor authentication, are being used more widely throughout the military, government, businesses, and consumer sectors, the selection and implementation of which authentication factors to require is typically defined by security policy. Security policy is in turn typically established by a security organization that may have no formal metrics or means to guide its selection of authentication factors. This paper will present a taxonomy for describing authentication factors including important attributes that characterize authentication robustness to aid in the selection of factors that are consistent with the user's mission. One particular authentication factor that I have developed will be discussed in the context of this taxonomy to motivate the need to broaden current definitions and security policies. The ultimate goal of this paper is to inspire the development of standards for authentication technologies to both support mission aware authentication innovation and to inform decision making about security policies concerning user authentication and authorization. Further, this paper aims to demonstrate that such an approach will fundamentally enhance both security and usability of increasingly networked, software-defined devices, equipment and software applications.

1. Introduction

Mobile devices, such as cell phones and tablets, can be extremely useful for military personnel, security personnel, employees, and consumers in performing an entire gambit of tasks from routine day to day tasks to time critical emergency response. Current cybersecurity best practices encourage the use of user authentication in order for these devices to be accessed. Increasingly, equipment that was once thought of as hardware, is becoming essentially software defined. This includes military radios, medical devices, and autonomous cars. This trend supports the possibility of requiring users to authenticate with their cars, medical devices, and radios, for example, before gaining access to their functionality, thereby enhancing security and discouraging theft and/or hacking. Further, Internet of Things (IoT) devices are becoming pervasive throughout homes and industries, and security policies for IoT device access have not consistently been established and implemented.

This paper is an extension of work originally presented in [1], where a method for continuous secondary factor authentication for military or security personnel required to perform missions while in harm's way was motivated and described. Specifically, this paper will use the Concept of Operation (ConOps) and method discussed in [1] and related ConOps to motivate the need for mission aware authentication factors and in turn to describe and validate authentication factors so that appropriate ones can be selected. This paper will further argue that standards and/or specifications and a means of validating compliance is crucial to support innovation and transition to productization.

In [2], the National Institute of Standards and Technology (NIST) defines multifactor authentication as "Authentication

* Corresponding Author: Susan Gottschlich, susan.gottschlich@raytheon.com

https://dx.doi.org/10.25046/aj020627

using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric)." When only two factors are used, this is referred to two factor or dual factor authentication. Dual factor authentication is currently a requirement for NIST's Risk Management Framework (RMF). RMF compliance is a requirement being levied on all military information systems.

Continuous authentication is an emerging authentication factor methodology that implements authentication as a process rather than a simple event such as entering a user name and password. The idea is that once a user establishes his or her identity through another authentication factor or as an initialization step in a continuous authentication factor, the user is continuously monitored by some means so that their identity is continuously established.

Continuous authentication can enhance usability by alleviating the need for a user to re-authenticate, for instance, if they allow their authenticated session to become idle for longer than some inactivity period prescribed by security policy. Continuous authentication can also enhance security by potentially detecting instantaneously when a user may have lost control of his or her device or software application session, eliminating the need for security policies to establish arbitrarily the length of inactivity periods allowed before re-authentication is required.

This paper argues that in order to enhance both security and usability, user authentication should be pervasively implemented on software-defined networked or stand-alone devices or software applications, but that the factors used in authentication should be selected to be consistent with the user's underlying mission and/or need for using the device or application. Thus, the factors employed may be far different than current approaches that typically involve entering a user name and password and/or pin along with a secondary factor (something the user is or has).

Section II will present background on current work on authentication factors and on biometrics which are increasingly being used to support 'something you are' authentication factors.

2. Background

Until recently, user authentication has pervasively been implemented via the use of a password or pin as a primary factor (something you know). If a secondary factor is warranted, several options for 'something you have' have been implemented including an RSA key, a CAC card, an email account, or a token. Alternatively biometric factors (something you are) such as finger prints, iris scans or voice spectrograms have been used. Section 4 will review ConOps examples where such approaches might not be practical given the user's mission.

Various implementations of an emerging authentication approach – continuous authentication – are beginning to emerge. Some of these implementations are described in industry publications [3, 4], and in conference proceedings [5]. Continuous authentication is the idea that a user is monitored in such a way that they are being continuously authenticated. An approach presented in [5], for instance, uses a combination of color information of users' clothing and face information in order to robustly monitor a user who may not always be facing the computer being used. Other continuous authentication approaches presented in [3, 4] use behavior recognition, such as keystroke patterns (e.g. typing rhythm, mouse movement) potentially used in combination with other biometric factors such as iris patterns.

Continuous authentication can bring about more secure authentication that is also more usable than current pervasive security policies implement. For instance, if a user who is not being continuously authenticated walks away from his or her computer briefly, a nefarious agent can assume this user's computer session. Locking computer sessions during inactivity periods is meant to counter this possibility but if the inactivity period is too short, it can become extremely counterproductive for a user who must frequently re-authenticate.

Alternatively, allowing for a lengthy inactivity period negatively impacts the security posture of the computer session. Continuous authentication is theoretically more secure because it tracks the user continuously, thus no timeout or inactivity period need be implemented. It may also be considered more user friendly because users do not need to re-authenticate.

An important thing to note about continuous authentication implementations is that they are generally tied to the type of device being used. For instance, key stroke and mouse behavior monitoring applies to computers but not necessarily cell phones or IoT devices. Further, they are often dependent on a user's mission or role. Tracking clothing, irises, and keyboard behavior are certainly appropriate for office and home environments. They may be less appropriate in environments where users are wearing uniforms (clothing is always the same color across users and days) and protective eyewear, using their devices occasionally while they perform other challenging tasks (e.g. driving, patrolling), or put into high stress situations that may alter their behavior or voice substantially.

In [1] I presented an approach that I developed that uses a fitness tracking device paired with a mobile device to continuously monitor a user performing potentially hazardous missions. This approach locks the mobile device if conditions suggest that the user is under severe duress (possible captured), dangerously wounded or killed. In other words, this approach monitors the user and when it detects that the user may have lost control of his or her device, it fails the user's authentication with the device. Otherwise, it allows a user persistent uninhibited access to the mobile device.

The novelty of the approach is based on the recognition that all of the conditions that suggest a user has lost control of his or her device will bring about a sudden change in the user's biometrics as monitored by the fitness tracking device. Because this is the case, the various biometric sensors can be monitored using Kalman filters which can detect jump (or sudden) changes in a biometric variable.

In [1] I describe experiments conducted with this continuous monitoring approach. The experimental results, which were derived from live experiments with 'normal' conditions but simulated experiments with dangerous conditions, confirm the approach's ability to provide strong authentication under the assumed user conditions.

As far as I am aware, this is only continuous authentication approach published that considers how to detect and lock down a device when conditions suggest that the user has lost control of his or her mobile device.

While this is generally not a concern for office workers or personal device users, it may be an important concern for military and security users. This differentiation further suggests the need for selecting mission-aware authentication factors.

When contrasted against NIST's definition of authentication factors, the fitness tracking device might be considered both something you have and a means to identifying something you are. In addition to tracking biometric readings, the fitness tracker's API also allows the authentication software to monitor band contact, so it is possible to detect when the user is no longer wearing the device or the tracker is no longer communicating. This paper will argue that combination factors and other innovations will be encouraged if security organizations are given the tools to evaluation their effectiveness.

Further, I submit that the emergence and commercialization of many new technologies including biometric feature sensing and recognition, wearable technologies, and machine learning (ML) will support more innovative and specialized approaches to user authentication.

There is substantial related literature on the biometric readings that might be drawn from in order to help assess the strength and risks associated with a biometric factor. In his Ph.D. dissertation, Gari D. Clifford discusses heart rate variability (HRV) and its causes [6]. Clifford shows that a person's heart rate is variably by nature. For instance, Circadian rhythms will drive variability throughout the day and factors such as general stress level and caffeine intake will cause day to day variations.

Several publications, including [7, 8, 9] consider heart rate variability, Galvanic skin response (which can be measured with some currently available fitness trackers), and other factors in analyzing what happens during exercise, duress, and the differences between the two. Based upon the research presented in [6-9], I developed rules presented in [1] to differentiate conditions that result in an increased heart rate.

Note that all of the biometric factors used in the algorithm in [1] can be measured by the Microsoft® Band 2, which was used in the experiments that were described. Skin conductance delta (also known as Galvanic skin response), for instance, supports the estimate of duress, but other factors can be used in differentiation. My research indicates that conditions resulting in a sudden decrease in heart rate (e.g. extreme cold, cardiac arrest) generally indicate the user is severely stressed by health or environmental issues, rather than an explicit threat.

Research presented in [10] performed a case study on students under stress due to a university examination. In [11] the use of wearable sensors is compared to electrocardiograms and concluded that the former is sufficient for detecting stress conditions.

Much of the research on heart rate measurements are focused on detecting an abnormal condition that may occur during a medical procedure such as surgery. The approaches discussed in such research generally involve preprocessing the measurement signal and performing machine learning (ML) techniques.

The algorithmic approach presented in [1] rejected the application of a pure ML techniques because measurable biometrics, such as heart rate, will vary from day to day due to many factors such as time of day, intake of caffeine or other drugs, and the user's current activity, and it is not practical to control for these factors.

Rather, the algorithm focuses on detecting jump changes in biometric measurements so that normal variances in measurements are implicitly handled.

The work in [12] describes the use of Electroencephalogram (EEG) for authentication. When mature, this technology may be trusted to uniquely authenticate an individual as a single factor (e.g. as opposed to dual factor or multifactor authentication). An unanswered question is how well these approaches work under high stress and maybe duress situation.

The work in [13] addresses biometric recognition techniques, including facial recognition, voice recognition, finger print recognition and iris recognition, being applied to authentication. It further describes how to assess biometric characteristics in terms of five qualities: robustness, distinctiveness, availability, accessibility and acceptability. The work further developed a taxonomy of uses. The focus of this work, however, is in 'snapshot' authentication – authenticating a user at a particular point in time using a snapshot reading (finger print, facial image, etc.) as opposed to the continuous streams of readings I proposed using in [1].

Nevertheless the discussion in [13] can easily be extended into the continuous monitoring domain if it can be assumed that there are mechanisms to continuously take snapshots of the discussed biometric factors.

In the following I will first propose a taxonomy for authentication factors that expands on the work presented in [13] in Section III. Specifically, I decompose the qualities presented in [13] into measurable and verifiable attributes. Further, these attributes are intended to support a broad array of potential authentication methodologies.

In Section IV, I present three ConOps to consider with regards to the taxonomy. I will conclude with a discussion of next steps.

3. Authentication Factor Taxonomy

The purpose of this section is to present a draft taxonomy for authentication factors and the user's that they are designed to identify and authorize. The goal is to motivate the development of industry and government standards organization that develops and maintains taxonomies and related standards that can be utilized by manufacturers of authentication devices and/or algorithms as well as security organizations or home users who must ultimately determine authentication policy. This draft has been developed informally as a means to motivate a formal taxonomy following a research methodology, for instance, as described in [14, 15].

The draft ontology is decomposed into three related groups of attribute/value pairs for describing authentication factors, user missions, and security policy.

Table I provides a list of key attribute/value pairs that can be used to provide specifications for an authentication factor. It is anticipated to be used by suppliers of authentication factors to provide an unambiguous description of the level of security a given authentication factor offering is able to support. It is also anticipated to be used by security organization to specify policy for the conditions under which a given methodology can be used.

This taxonomy can be seen as an extension of the characterization described in [13] because it encompasses the full range of authentication factors and it including attributes that might be used in a risk analysis (e.g. some connection protocols may be considered to be less secure than others). It further attempts to decompose the qualities into attributes that are measurable and verifiable.

This taxonomy strives to address current and emerging authentication methodologies. It is understood that future innovations may bring about methodologies that will require a further extension in the taxonomy. Nevertheless it is quite possible that future innovations will not change the attributes in the taxonomy but instead extend the range of potential values associated with each attribute.

It is the only taxonomy that I am aware of that is meant to model emerging authentication factor technology including continuous authentication and combination factors (e.g. something you have and something you are). I believe that research aimed at characterizing authentication factors is essential to promote innovation in authentication factor offerings. Without such a mechanism, innovators may have a hard time determining whether or not a proposed authentication concept will, if developed, be acceptable by security organizations and users, and thus less likely to expend resources developing innovative authentication approaches.

The first attribute, category, provides a high level simple characterization. Security policies may use this characterization to structure the definition of acceptable authentication factors. In turn, users may use it to determine the best factor(s) to implement their ConOps.

Table 1: Authentication factor definition

ATTRIBUTE	VALUE
Category (structure which provides high level distinctions to support policy definition)	-Discrete, continuous, or continuous with initial discrete authentication factor -Something you know, something you are, something you have, or a combination factor.
Strength (structure that varies depending on the underlying factor)	-Something you know: number of characters, special characters (for single entry), number of questions (for security question knowledge based authentication) -Something you have: restrictions on how the device is obtained, if/when it expires, policies for how lost, stolen, or damaged devices are replaced - Something you are: frequency of interrogation
False Acceptance Rate	Expressed as a percentage. May be calculable based on strength settings.
False Rejection Rate	Expressed as a percentage. May be calculable based on strength settings.
Validation Approach	The approach used to validate strength, false acceptance rate and false rejection rate established.
Connections required (something you have, something you are)	Wired interfaces including: USB, DS-101. Wireless interfaces including: WiFi, Bluetooth, ZigBee (IoT), Proximity card, Near-Field Communications (NFC)
Acceptable user conditions	A list of well-defined conditions including: Continuous use, continuous use with occasional interruptions, wearable-occasional use, pocketed-occasional use, protective face equipment, protective eye equipment, protective hand equipment, protective finger equipment, exertion-tolerant, stress-tolerant, voice use, covert use.
Authenticated devices and applications	A list of well-defined devices, including computer (keyboard, mouse, camera), tablet, phone, software defined equipment, IoT device, etc.as well as applications that the factor can support.
Acceptable devices for authentication factor (if required)	Varies depending on the factor (e.g. USB token, wearable device, software algorithm to run on device for use).
Additional events detected	A list of well-defined events including: duress, medical issue, fatigue, theft, tamper.

The next three attributes – strength, false positive rate and false negative rate – aim to support objective measurable specifications that address the 'robustness' and 'distinctiveness' qualities described in [13]. The strength attribute represents methods by which an authentication factor can be configured (from a supplier's point of view) or must be configured (from a security policy point of view). The strength attribute is particularly important for something that you know factors (e.g. passwords). For continuous factor authentication, strength may be described in terms of the sampling rate (how frequently classification/recognition is performed). For knowledge-based authentication (e.g. answering security questions), strength may be described in terms of the number of questions required to authenticate. The strength attribute is usually configurable.

False acceptance rate and false rejection rate are important for biometric and continuous authentication factors. They are specialized from the universally accepted receiver operating characteristic (ROC) curve mechanism for statistically characterizing the sensitivity and specificity of a binary classifier (for instance see [16]).

In the realm of user authentication, these measures are intended to capture statistically how likely a false user successfully authenticates or a true user fails to authenticate. This occurs because biometric recognition technologies (face recognition, voice recognition, etc.) are not perfect. Specifically, distinctiveness is addressed by false acceptance rate. A low false acceptance rate suggests that the underlying algorithm is able to distinguish a true user from false users.

These attributes are extremely important in helping to select which of perhaps many similar technologies is appropriate for a given application. They may not, however, be meaningful for more traditional authentication factors (e.g. something that you know) such as passwords as there is virtually no way for these factors to be misrecognized.

False acceptance and rejection rates are usually not directly configurable. However, it is frequently possible to tune them. For instance, lower false acceptance rates may be achievable by tuning algorithmic parameters in such a way that the false rejection rate increases as a result. Other factors, possible tied to strength, might also be tuned to decrease these rates. For instance, acceptance rates may increase or decrease depending on the frequency of classification/recognition.

The validation approach attribute is important in specifying how strength and acceptance rate specifications are validated. False acceptance rates and false rejection rates quotations may be very low if, for instance, statistical validation is performed using a small homogeneous sample set. Further, the validation approach may help a security organization determine under which conditions an authentication factor may be useful. For instance, voice recognition technologies may be robust in quiet lab environments but less so in outdoor public environments. This attributes addresses, in part, the acceptability and accessibility qualities from [13].

The connections requirement is particularly important for security organizations that need to perform a vulnerability analysis. Any connection interface is potentially vulnerable to exploitation, spoofing and/or denial. Further, organization may have implemented mechanisms for minimizing vulnerability for given connection types and thus prefer some technologies over others. Note that this attribute may not be relevant to 'something you know' authentication. This attribute addresses, at some level, the availability, accessibility, and acceptability qualities from [13].

The acceptable user conditions attribute supports the acceptability and accessibility qualities. Emerging authentication factors will likely be specialized for a given user condition or situation in order to support appropriate robustness while also maximizing convenience. For instance, continuous authentication based on facial recognition is only appropriate in situations where the user is expected to always be facing the face image capture component of the authentication factor. This may be appropriate for continuous use of a computer in an office environment, but may be less appropriate for occasional use devices that are frequently pocketed.

The next two attributes Authenticated devices and applications and Acceptable devices for authentication factor are simply characterizations of the equipment/software that a factor is intended to authenticate (e.g. computer, bank account session) and equipment used to perform the authentication. These attributes anticipate that suppliers may want to provide software-based solutions that can run on a variety of equipment. For instance, a factor that involves the use of a fitness tracker could potentially run on a variety of commercially available trackers. Thus, this attribute addresses the 'accessibility' quality discussed in [13].

Finally, the additional events detected attribute formalizes the concept that many potential authentication factors may have applications well beyond that of simple authentication. In particular, continuous biometric authentication factors may be able to detect events not directly related to authentication or security such as health events or fatigue. This attribute addresses the 'acceptability' quality from [13]. In particular, an organization may be more willing to invest in an authentication factor approach if it may bring additional benefits beyond robust authentication.

It should be noted that Table I is used to describe 'opt in' technologies where the user has opted to use an authentication factor in order to identify themselves. In biometric recognition and related areas, 'opt out' technologies are used to identify individuals without their direct compliance. While opt out technologies define an important research area, I do not believe that they are appropriate for authentication factors as most current uses for authentication implicitly involve users opting in in order to utilize the equipment or service being secured.

To achieve security policies that are appropriately flexible while maintaining a strong security posture, it is important to take into account a user's mission. In many situations today, security policies only allow a single combination of authentication factors. The result is that users may not use equipment or services that is too onerous to access, may seek mechanisms to subvert the security policies decreasing the security posture, or may put up with the inconveniences reducing their overall effectiveness and safety. Future security policies might allow a user community to select their own factors and instead provide guidance on how the selected factors must be configured and used in order to be allowable.

Toward this end, Table II provides a draft taxonomy for users in the context of the mission they are performing and for which they need devices and applications authenticated. It is anticipated to be used by a mission leader. The first attribute, mission class, is intended to be a high level characterization to simplify selection and guidance of authentication factors.

Table 2: User (Mission) Definition

ATTRIBUTE	VALUE
Mission Classes	A list of well-defined mission classes including: Desk worker, Office worker not at desk, Factory worker, Home indoor user, home outdoor user, tactical user in hazardous situations, tactical user not likely in hazardous situations, tactical user in extreme environments, etc.
Anticipated session duration	Varies but used to help determine how often a user might be required to re-authenticate
False Acceptance Rate tolerance	Taken together these might be used to select appropriate factors and/or their configurations. For instance, a factor may be configured for extremely low acceptance rate while allowing higher rejections rates (possibly forcing user re-authentication)
False Rejection Rate tolerance	
Acceptable user anomalies	A list of well-defined conditions that are acceptable for a user to exhibit during a valid authentication session including: Stress, strenuous activity, covert use, extreme environmental conditions, etc.
Mission restrictions and conditions	A list of well-defined restrictions and conditions including: outdoor use, wired and wireless restrictions, etc.
Devices and/or applications requiring authentication	A list of devices or applications including computer, tablet, phone, software defined equipment, IoT devices and web site account sessions.
Authentication factor limitations	A list of well-defined restrictions including: no-keyboard requirement, no carry requirement

The second attribute, expected duration, is important in selecting technologies and methods. For instance, more rigorous initialization and/or calibration steps may be more acceptable for long duration uses. If the duration is anticipated to span multiple days then authentication approaches must deal with users sleeping and bathing. For some technologies, expected battery life on equipment is an important consideration.

False acceptance and rejection rate tolerances are important in helping mission leaders specify acceptable risks. For instance, a mission leader may need to consider the risk of an authenticated device falling into an adversary's hands. To the extent that recognition algorithms are tunable, a mission leader may insist on a tuning that is either very conservative for false acceptance rate or very conservative for false rejection rate.

Mission restricts and conditions are important for helping users consider what authentication technologies may be acceptable. Outdoor usage suggests weatherproofing and often battery operation. Wireless transmissions are ultimately observable and/or disruptable by an adversary, but some are less so than others.

Listing all of the equipment or services that a user might authenticate with in order to carry out their mission may spur the usage of authentication factors that can be applied to multiple devices simultaneously. For instance, a wearable device may potentially interface with all of the equipment a user may need to use during a given mission so that they are less encumbered by individual specific authentication processes.

Authentication device restrictions may be used to reject authentication factors. Something you have factors such as tokens or cards are problematic if a user damages, loses or forgets to bring them, particularly where there may be no viable back up options. This case may suggest a 'no carry' restriction. Users wearing protective hand gear may reject any approach requiring a keyboard or keypad.

Table III is intended to allow a mission leader to work with a security organization to develop appropriate security policies and to allow the mission leader to determine how best to perform his or her mission given acceptable risks. A security policy may allow a variety of primary factors to be used as long as they meet requirements spelled out in the security policy. The same should be possible for secondary factors. A supplier offering an authentication factor that is intended as a secondary factor might provide appropriate interfaces to a variety of primary factors in order to facilitate integration.

As wearable devices and biometric recognition algorithms become more capable, I believe that it should be possible to develop an authentication factor that can be used to 'unlock' a number of devices or services. In particular, software defined equipment could interface with other equipment to obtain authenticated user credentials providing a stronger security posture without placing additional requirements on the user.

Thus, future security policies should define to what degree they will allow multiple simultaneous devices and/or applications to be authenticated by a given authentication factor or combination of factors. Today, a similar concept is in common use, referred to as single sign on, where once a user authenticates with their computer, for instances, their credentials are made available to software applications (avoiding the need to re-authenticate).

Table 3: Authentication Policy definition

ATTRIBUTE	VALUE
Primary factor requirements	Restrictions on the primary authentication factor. These requirements should specify restrictions on strength and mechanisms for re-authentication if ‘something you know’ is forgotten or ‘something you have’ is misplaced, forgotten, or damaged. It may further provide restrictions on secondary factors paired with it.
Secondary factor(s) requirements	Restrictions on the secondary factor(s) (can be more than one). Includes re-authentication mechanisms, restrictions on strength
Acceptable devices or services for use	A list of devices or services that can be simultaneously authenticated via a single (multifactor) authentication.
Anomaly policy	A list of well-defined actions to be taken including logging, notification, etc.
Rejection policy	A description of what happens when user authentication is rejected including logging, notification, locking session, etc.
Recovery policy	A description of how a valid user ‘recovers’ from authentication factor issue including forgetting information, losing, damaging or forgetting tokens, biometric measurement issues, etc.

Anomaly policy provides guidance on what actions are taken if anomalies are detected. For instance, an anomaly on a user’s tablet might trigger a notification to the mission leader that might help the leader decide whether or not to take action.

Finally, rejection policies in the future may be more flexible than they are today. If a user loses control of their device, it may make sense to lock or even zeroize the device. However, if the possibility exists for them to regain control, a policy that might allow partial access to emergency features (e.g. ability to send emergency requests to a mission leader) or re-authentication features.

Note that Table I-III are not meant to be completely exhaustive. Rather their intent is to trigger discussions about how to completely define authentication technologies vis a vis user missions and security policies so that standards and/or specifications can be developed that are inclusive of a wide range of authentication technologies.

While the scope of situations for which this taxonomy is intended to address is extremely wide, Table IV attempts to outline a potential approach to using the three part taxonomy presented in this section to select an appropriate authentication methodology for a given mission.

4. ConOps and Authentication Limitations

To better motivate the need for innovation and flexibility in authentication factors and the security policies used to provide restrictions and requirements for them, this section will describe 2 ConOps for which currently acceptable assumptions made about authentication implementations may not hold and 1 for which they do.

The first ConOps was originally presented in [1]. Here a tactical user, such as a soldier, Marine, law enforcement officer, guard or emergency responder, uses a network-enabled cell phone or tablet to support their operations. The user’s device might be of critical importance in helping them identify and locate persons of interests or threats, send out requests for back up or exfiltration, or report back relevant intelligence and observations.

The challenge here is that user authentication is extremely important to insure that if the user’s device or they themselves are captured by a red force actor (enemy combatant, criminal, or other threat) that the red force actor is not able to exploit the device to gain access to critical information and/or intelligence. On the other hand, the user authentication should allow the tactical user uninhibited access to the device up until the moment that the tactical user loses control of it.

A fundamental assumption that we made in pursuing this work is that the target user community can be characterized by the following constraints:

- The user needs to access their device even when they are in harm’s way and there is a possibility that the device may fall into the hands of adversaries including insider threats.
- The user will need to access their device while performing other tasks that will take precedence over device interaction.
- These may include driving, surveilling or monitoring, or physically interacting with civilians, criminals or other red force actors.
- Thus, authentication factors tied to inactivity periods are not practical as the tactical user may be inactive, vis a vis the device, throughout the majority of their tactical mission.
- The user may want to be able to access sensitive data and applications covertly (for instance, if they are undercover).
- This implies the use of commonly available devices, not specialized restricted equipment.

Table 4: Selecting Authentication Methodology for a Given Mission

CONSIDERATION	TAXONOMY RELEATIONSHIP	COMMENTS
What devices and/or applications are required for the mission and do they need to be protected?	Table II – Mission class, expected duration, devices and/or applications requiring authentication	Include the following: • Software defined equipment (e .g. radios, networks, sensors) • Applications running on computing devices such as computers, tablets, phones Consider if it is possible to implement authentication directly into the device or application: • Can authentication be added to or credentials shared with software defined equipment? • Can authentication be added to applications? Consider if alternative mechanism to protecting devices is possible: • Physical device not require protection but cloud based applications running on them do need to be protected. Is there an effective mechanism for authentication on the cloud? • Software defined equipment does not need to be protected as long as the infrastructure that it integrates with is able to provide protections
Risk of false acceptance	Table II - False Acceptance Rate tolerance	If a red force actor gains access to mission devices and/or applications, what are the risks (critical information access, ability to reengineer underlying technology, ability to perform malicious actions with capture devices and/or applications)? Are there other mechanisms to mitigate the risks?
Risk of false rejection	Table II - False Rejection Rate tolerance	If a user can no longer access their devices and/or applications, what are the issues (inability to communicate with teammates, inability to navigate mission area, loss of knowledge access critical to perform mission, inability to perform actions required for mission). Are there other mechanisms to mitigate the loss of access?
Restrictions on authentication factors	Table II - Authentication factor limitations	Consider if a user can use their fingers at all times that device interaction is required. Consider if a user can wear a device and where (wrist, finger, around neck). Consider if a user may forget something they know. Consider if a user may loss, damage, or forget something they have. Consider if a biometric feature will be available to measure (iris scan, finger prints).
What category(s) of authentication methodology are acceptable	Table I – Categories	Work with Security organization to find categories for which policies exist or develop new policies for given category.
What is the best authentication implementation?	Table I – Remaining attributes	Work with Security organization to select authentication factors and configurations to meet mission requirements and provide appropriate protection.
How to implement security policy?	Table III all attributes	Work with Security organization to determine how best to implement policy to provide appropriate protection and mission flexibility.

- The user's organization does not wish to waive cybersecurity controls associated with identification and authentication because the cybersecurity risk of the waiver is considered higher than is acceptable.

To support this ConOps, we developed a continuous authentication algorithm for monitoring the availability of a fitness tracker, worn by the user, and connected to the device via a consented Bluetooth wireless connection. The algorithm further estimating a user's health status based on biometric sensor readings read from the fitness tracker. In particular, we implemented the algorithm using both a Microsoft® Band 2 and Microsoft® Band 1 fitness tracker connected to a Microsoft® Surface tablet.

While the ultimate use of the proposed algorithm must be determined by the security policies of the organization responsible for managing the mobile devices, the proposed use of the algorithm is to provide a continuous stream of user health status estimations to be used as a secondary authentication factor. Certain statuses, when they are identified, will cause the device to lock and/or wipe sensitive data depending on organizationally defined procedures. In particular, the following situations may indicate authentication failure or partial failure limiting device access, especially to sensitive data:

- The fitness tracker loses contact with the wearer or the connection with the device implying that the user may no longer have his or her device and/or fitness tracker.
- The tactical user is under extreme duress implying that the user may no longer be in full control of the device or may be being manipulated by the threat.
- The tactical user may be dead or their health may be extremely compromised indicating that the user is unable to maintain control of the device.

In [1] we presented a jump Kalman filter (JKF) that continuously monitors the fitness tracker sensor readings looking for 'jump' discontinuities that might indicate one of the above three situations. Jump discontinuities are required to differentiate between, for example, duress and extreme physical exertion, the latter being an acceptable and even expected situation for the tactical user.

The benefit of using JKFs over explicit ML techniques is that JKFs are always using recent history to predict a user's next biometric reading. As long as the biometric readings do not change suddenly, the JKF's estimates will be very close to the actual readings. At times when the variability of the readings is high, the estimated covariance is high, so the allowable difference between the estimates and actual readings is increased. It is only when a true discontinuity in readings is observed that a jump is identified. This means that regardless of what a user's health state is after the user is initially authenticated by whatever means, as long as it does not change suddenly during the continuous monitoring, the JKF does not recognize a duress or other disqualifying condition. See [17,18] for other work related to JKF algorithms.

ML techniques can be very powerful, but many will require an initial training period. This may require retraining during every authentication session when using sensor readings or outputs that change a lot over time, e.g. from day to day. Of course, if the degree of difficulty involved in retraining is low, ML techniques might be very useful.

The implementation of the JKF algorithm and its configuration can be used to illustrate important considerations in user authentication. Ultimately, for a security organization to trust such an algorithm, they should require objective metrics on its performance in all relevant conditions. These include probability of false acceptance and probability of false rejection. Ideally such metrics might be computed by a supplier of this kind of authentication factor but then an important question is how these metrics are collected. Ultimately, it may be difficult for a commercial organization to thoroughly vet such an algorithm with actual users because it might require putting users into, at least convincingly, dangerous situations.

Further, this algorithm performs best when calibrated. Kalman filters normally are calibrated by simply collecting a small amount of history at the beginning of a session. In [1] we used 10 seconds of history to calibrate the JKFs. Jumps were recognized by the difference between actual and predicted readings exceeding the filter's covariance by greater than a predetermined constant factor:

$$|\boldsymbol{x_k} - \boldsymbol{z_k}| > C\,\sigma_z{}^2 \qquad (1)$$

where $\boldsymbol{z}_k$ is the measurement, $\boldsymbol{x}_k$ the prediction, $\sigma_z{}^2$ the covariance, and C is a predetermined constant factor. One potential use of ML in conjunction with a JKF is in establishing the value of C, which may or may not be a constant. For instance, it is possible to imagine that the value of C may be best expressed as a function of other variables including the covariance. Ultimately, rigorous calibration mechanisms that are not unduly onerous for the user community are needed and security organizations need confidence in these mechanisms.

It should be noted that in addition to supporting user authentication, the approach presented in [1] supports a host of auxiliary requirements and features, including enhanced situation awareness of tactical users' status, early indicators of conflict or environmental hazards, and possibly early warning of health related issues (e.g. experiencing duress when not in a hazardous situation). It is likely that many of the other approaches being invented for user authentication might also be capable of supporting ancillary features.

A second ConOps is that of a tactical user, such as an Airman conducting an airborne mission. In such missions, physical access to mission aircraft is heavily restricted by armed guards. Because of this, in the past, authentication requirements may have been waived. In recent times, however, concern over insider threats, which may be inadvertent, accidental or deliberate, have forced tactical users to perform dual factor authentication. User authentication both limits access to the aircraft systems to trusted users and enforces nonrepudiation – the concept that an authenticated user cannot perform an action and later deny it.

An issue with requiring 'something you have' such as a token as a secondary authentication factor in such situations, is that if a user forgets, losses, or damages the card it may be necessary to scrub the mission.

Biometric factors may be complicated by the requirement to wear personal protective equipment. A further concern with biometric factors, such as finger prints, is that a red force actor can physically force a user (conscious or unconscious) to provide a reading to the authentication system.

One authentication approach for the tactical user that I believe will support strong security while alleviating concerns over authentication factor requirements involves a continuous authentication factor. Similar to the approach presented in [1], a continuous authentication factor tied to something that a tactical user may normally be wearing, such as a fitness tracker, may be used to establish and maintain the user's identity.

Further, this wearable device may be used to establish connections with all of the devices, such as radios and mission computers that the user needs to interact with in order to conduct their mission. The user could be automatically authenticated to all devices as long as the continuous authentication and connection to the devices remains viable. The continuous authentication algorithm used to establish the user's identity and continually monitor the user may be changed to reflect different aspects of the mission than the one described in [1].

Wireless technologies are frequently disallowed in classified environments which may include mission aircraft. In order to use a continuous monitoring approach such as the one suggested, either a wired device would be required to monitor the user, or a wireless protocol that is not considered vulnerable must be utilized. Bluetooth, ZigBee (utilized in IoT devices), or Near Field communications (NFC) protocols are probably the most practical for such situations but they may require further encryption or other restrictions before they are allowed in a classified environment.

A third ConOps to consider is one that is implicitly addressed in much of the literature involving continuous authentication. It is that involving a knowledge worker who is usually using a computer or tablet. During the course of a normal day's work the worker would not be expected to undergo severe stress or duress. Any such situation would be considered abnormal and would warrant locking the worker out of their session until he or she reestablishes it via more traditional means such as requiring the entry of a password or PIN or calling a help desk. In this situation, video analytics using the computer or tablet camera, keystroke behavior, or a variety of other factors are likely practical to support strong and usable security.

5. Next Steps

This paper has sought to demonstrate that an increasingly networked software-defined technology footprint in our work and leisure environments is expanding the need and/or opportunity for user authentication before allowing access to computers, phones, IoT devices, services, and general equipment. At the same time, technology advances in wearable devices, biometric sensors, behavior analytics and a host of other fields is supporting the potential for more secure and less onerous authentication methodologies. Developing innovative new authentication factors to the point of productization and mass production, however, will be accelerated if inventors, investors, and manufacturers understand that security organizations and even home users will accept alternative authentication factor technologies to the relatively simplistic ones commonly utilized today.

Toward this end, this paper has attempted to motivate the formation or expansion of a standards body concerning user authentication technologies and policies. The taxonomy presented in Section III is primarily meant to provide early talking points in the formulation of a standards or specification body.

In one somewhat related example of how standards bodies can spur innovation and technology development, the U.S. National Security Agency (NSA) developed and published the Commercial Solutions for Classified Program (CSfC) specification [19]. Manufacturers and solution providers have used this specification to develop capability sets that they in turn have been able to have registered with NSA after providing evidence of compliance with the CSfC specification. This allows third parties to purchase and integrate compliant capability sets into their environments. In the end, the overall process of getting a classified environment certified by NSA has become far more flexible, affordable, and expedient because of the specification and associated registration process.

A similar approach applied to user authentication may ultimately support stronger and less onerous user authentication, and it may further support the expansion of user authentication and access restriction's use within an overall cybersecurity plan further enhancing security and usability at an enterprise level. For instance, if all equipment in a factory, office, or military platform required user authentication to read and/or modify equipment settings and/or to use the equipment, it may be much more difficult for the equipment to be 'hacked' because network penetration alone does not provide access to the equipment and software running on it.

While such an approach may seem unacceptable today, acceptance of emerging authentication methodologies will increase within security organizations as their strength and acceptance rates are proven and their risks are understood and mitigated. Further, acceptance within user communities will increase as authentication processes become simpler and less prone to error.

Similarly, user authentication techniques that are easy to understand and utilize might be used to enhance home security in a consistent and predictable fashion reducing deliberate and/or inadvertent actions causing harm to occupants and/or damage to or loss of property.

Conflict of Interest

The author declares no conflict of interest.

Acknowledgment

This work was funded in part by Raytheon Internal Research and Development (IRAD) funds.

References

[1] S. Gottschlich, "Incorporating health monitoring and duress detection into mobile device authentication" in 2017 IEEE International Symposium on Technologies for Homeland Security

[2] Joint Task Force and Transformation Initiative, "Security and privacy controls for federal information systems and organizations" NIST Special Publication 800 (2013): 53

[3] B. Violino, "Continuous authentication: Why it's getting attention and what you need to know," in CSO, Mar 14, 2017

[4] R. Walters, "Continuous Authentication: The future of Identity and Access Management (IAM)" in Network World, Sep 16, 2016

[5] K. Niinuma and A. K. Jain. "Continuous user authentication using temporal information" in Proceedings SPIE, 7667(1), 2010.

[6] G. D. Clifford, "Signal processing methods for heart rate variability," Diss. Department of Engineering Science, University of Oxford, 2002.

[7] http://scienceline.org/2007/06/ask-hsu-fightorflight/.

[8] S. Boettger, V.K. Yeragani, L. Donath, H. J. Müller, H. H. Gabriel, K. J. Bär, "Heart rate variability, QT variability, and electrodermal activity during exercise" Med Science Sports Exercise 42(3), 443-448, 2010

[9] D. K. Spierer, E. Griffiths, T. Sterland, “Fight or flight,” The Tactical Edge, Summer 2009.

[10] P. Melillo, M. Bracale, L. Pecchia, “Nonlinear Heart Rate Variability features for real-life stress detection. Case study: students under stress due to university examination” BioMedical Engineering OnLine, 10(1), 96, 2011

[11] J. Choi, R. Gutierrez-Osuna, "Using heart rate monitors to detect mental stress" in IEEE Sixth International Workshop on Wearable and Implantable Body Sensor Networks, 219-223, 2009

[12] R. J. Rodriguez. “An Electroencephalogram (EEG) Based Biometrics Investigation for Authentication: A Human-Computer Interaction (HCI) Approach,” Doctoral dissertation, College of Engineering and Computing, Nova Southeastern University, 2015.

[13] J. Wayman, A. Jain, D. Maltoni , D. Maio, “An Introduction to Biometric Authentication Systems,” in J. Wayman, A. Jain, D. Maltoni, D. Maio, (eds), Biometric Systems. Springer, 2005.

[14] R. C.Nickerson, U.Varshney, J. Muntermann, “A method for taxonomy development and its application in information systems,” European Journal of Information Systems, 22(3), 336-359, 2013

[15] A. Hevner, S. Chatterjee, Design research in information systems: theory and practice (Vol. 22), Springer Science & Business Media, 2010

[16] T. A. Lasko, J. G. Bhagwat, K. H. Zou, and L. Ohno-Machado, "The use of receiver operating characteristic curves in biomedical informatics" Journal of biomedical informatics, 38(5), 404-415, 2005

[17] A. K. Fletcher, S. Rangan, and V. K. Goyal, "Estimation from lossy sensor data: Jump linear modeling and Kalman filtering" in Proceedings of the 3rd international symposium on Information processing in sensor networks, 251-258, 2004.

[18] L. Galleani, Lorenzo, P. Tavella, "Detection of atomic clock frequency jumps with the kalman filter" IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control, 59(3), 504-509, 2012

[19] National Security Agency, “Commercial Solutions for Classified,” available: https://www.nsa.gov/resources/everyone/csfc