Developing Coercion Detection Solutions for Biometric Security

Peter Matthew
Department of Computing
Edge Hill University
Ormskirk,
Email: peter.matthew@edgehill.ac.uk

Prof. Mark Anderson
Department of Computing
Edge Hill University
Ormskirk,
Email: mark.anderson@edgehill.ac.uk

***Abstract*—Biometric security depends on its accuracy and efficiency, but is especially vulnerable to spoof attacks. Currently liveness detection has become the standard method of reducing the impact of spoof attacks, however whilst this protects against spoof creation and presentation, it does nothing to detect legitimate users being coerced into accessing systems. This paper looks at this coercion concept, indicating the impact coercion could have on biometric security and how it can be detected. This paper will identify scenarios in which coercion detection could improve security as well as identifying the underlying concepts that make this area up, culminating in the presentation of four high level techniques which can be implemented within a multimodal biometric system to detect coercion detection.**

Keywords*—*Affect testing; Biometric fusion; Biometric security; Coercion detection; Threat vector analysis.

I. Introduction

Coercion detection is a currently an underused but necessary component of biometric security. Currently, there are no methods of detection if a user is being coerced into authenticating. If an attacker coerces a legitimate user to authenticate into a secure system, then they will bypass all of the intruder detection facilities that may be in place, subsequently making any spoof detection techniques employed irrelevant. The current process of biometric authentication revolves around the collection of a sample that is then processed until a decision to either accept or reject the user has been made. One of the main techniques to bypass this process is the use of spoof samples, which are presented to the system during the sample collection stage of authentication. These spoof samples allow non-authorised users to access the system by using a sample stolen from a legitimate user, therefore bypassing many security techniques. Liveness detection was formed to address this spoof threat and minimises the impact of sample theft and presentation. However sample theft and spoof development deals with spoof provision, and is checked after the user has already provided their data to the authentication process. This paper focuses on what will occur if a legitimate user is coerced into providing their authentication details to the system. This problem occurs at the start of the authentication procedure and has the potential to render other security techniques, such as liveness detection, inconsequential.

II. Coercion Scenarios

To coercion a user, is to force them to do something they do not want to do by using threats and/or force. Therefore during the process of coercion the psychological factors, of the user, will change depending on the situation. It is these physiological factors that can then be gathered and analysed to denote if coercion is occurring during an authentication attempt.

Regardless of how coercion is measured, the first question would be to denote if a coercion detection technique would benefit biometric security. The following provides some basic scenarios that would benefit from this addition to the technology.

1) Banks and shops have access to vaults and tills which are choice targets for thieves. The official UK definition of robbery is "A person is guilty of robbery if he steals, and immediately before or at the time of doing so, and in order to do so, he uses force on any person or puts or seeks to put any person in fear of being then and there subjected to force" [1]. In the UK 2014 there was 40,000 cases [2] of robbery. However, the inclusion of integrated biometric security and coercion techniques, on vaults and cash registers, would reduce the number of robberies as it would be harder for employees to access the devices during coercion. This is because the employee, during a robbery, is forced to aid the perpetrator by providing the goods or by accessing either the vault or till, as they would have the correct biometric authentication to do so. However, if a coercion techniques such as facial muscle movement is used to denote coercion then the authentication process can be halted, and the attacker will be denied access. Similarly, shop tills could be equipped with skin conductivity coercion techniques, within fingerprint authentication systems, that would prevent staff opening the tills if coercion is detection, again preventing the attacker access to the system.
2) Due to the risk of terrorism and the disasters that have occurred over the past decade and a half, the inclusion of secure coercion biometrics would prevent attackers accessing transport controls. There have been ten plane hijackings, ignoring corporate jet and military transports, since 2010 [3]. The inclusion of coercion techniques could prevent a hijacker accessing the cockpit, or another control centre on transports such as trains or boats. This is especially pertinent when considering naval travel, as piracy is one area that has been increasing significantly [4] in the last decade.

Therefore, the inclusion of coercion detection on bridges that would minimise the effect of piracy by not allowing attackers access to the control area by forcing an authorised user to authenticate.

As these examples show the inclusion of coercion detection techniques could help prevent illegal access to a variety of systems. The next question is to identify where coercion detection would be best implemented. This will be done by identifying the threat vectors for coercion detection, and identifying where best to implemented coercion detection methods. Therefore, the identification of coercion based threat vectors will allow pertinent defence measures to be developed that will improve the overall level of security for biometric authentication. Practically this could reduce the ease in which attackers coerce authorised users into authenticating and could minimise factors such as hijacking, vault robberies, etc. Subsequently, the purpose of this paper is to identify where the threat vectors occur during the biometric authentication process and what methods of minimising these vectors can be identified. These prevention techniques will be discussed regarding their threat vector minimising impact.

III. Current Threat Vectors

The original method of identifying threats to biometric systems was to highlight the areas of vulnerability that occurred during the authentication process. This has been documented thoroughly by [5] [6] [7] amongst others and each iteration has highlighted more threat vectors to content with as demonstrated by Figure 1 which identifies four specific threat areas.

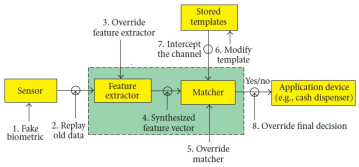

Fig. 1: Expanded threat vectors based [8]'s work

[8] identified four areas in which attacks might occur which are; user interface attacks, inter-modal attack, module attacks and template database attacks which are shown in Figure 1. User interface attacks involve the use of a fake or spoof biometric characteristics which such as the gummy fingers technique, HD imagery and so on [9] [10]. The second vector addresses the potential security issues that occur during the communication process between different modules/entities within the authentication process such as remote interception of signals or from a local jammer/interceptor. These attacks are conducted by nefarious users who substitutes their signal that can result in sample manipulation or by changing the location of a correct template and replacing it with a spoofed template. The third attack is a Trojan Horse like attack that creates a backdoor into the system. This allows the attacker to execute their code regardless of previous security provisions. However this can be countered by including secure software practices and the inclusion of specialised hardware/software which will improve the chance that the algorithmic integrity of the process is maintained. The fourth attack vector details attacks related to the template database and has the potential to be one of the most devastating attacks as the template database is where all of the enrolment samples are kept ready for matching. There are some issues that can arise from this kind of security breach: it allows the attacker to substitute a spoof biometric template with one that contains the attackers, or their representatives, sample. Subsequently, this gives the attacker the ability to access legitimately the system (from the system's viewpoint) or the ability to create an official template, therefore, creating a legitimate way into the system that does not rely on the initial attack, therefore becoming harder to both trace and solve.

These threat vectors highlight the base biometric vulnerabilities however this does not necessarily mean that the same vectors will be more or less important for coercion detection. Therefore the identification of any coercion centric threat vectors, and any methods of reducing these threats is paramount to minimise the effects on the overall security. If these vectors are not considered then attackers will have a much easier method of bypassing system security potentially leading to a greater quantity of coercion based attacks. The next section will identify where coercion can create a threat vector, new or current, and will lead on to proposing techniques to minimise these vectors.

To begin this process the definition of coercion was sought so that it could be kept at the forefront of development. "To persuade (an unwilling person) to do something by using force or threats"is how [11] describes coercion. When considered in context, this means to force an unwilling user to utilise their biometric sample to gain access to a system, therefore bypassing the main security and liveness methods as the sample used is valid. Therefore, how will it be possible to detect if a user is being coerced into a system? To identify this the following questions have been considered:

1) What current threat vector are there for coercion [8]?
2) What coercion attacks can be used?
3) What coercion detection techniques need to be developed?

A. Coercion Threat Vectors

Due to the user centric method of system breaching, coercion techniques focus heavily on the sample provision/sensor stage of the biometric process. This is because to coerce a user, the attacker must force the user to provide something. In this case the authorised sample and this is only done at the sensor layer. However the whilst this is the main threat vector the potential solutions can work at different stages within the overall biometric process. This would depend on what technique of coercion detection was being provided voluntary or involuntary.

When considering coercion the primary method of detection is gathering and analysing the physiological changes associated with specific emotional responses. The primary of which being fear, but other similar emotions such as stress and disgust can also be used. These can be gathered at a very high level as [12] postulates saying that when using functional magnetic resonance imaging healthy humans, required a negative connectivity with the cortical and subcortical pathways towards the amygdala (set of neurons within the temporal lobe) therefore potentially enabling fear to be detected. However, while it may be possible to detect fear

in this manner, the technique required would prove prohibitive within most installations, except in extreme circumstances, due to the cost, implementation difficulties and acceptance of the technique.

As already mentioned the main area of threat is the sample provision area. This is because if an attack is based elsewhere then it will be handled by other factors, such as temple protection schemes, encryption liveness detection etc.

To highlight this a work flow for a coerced authentication has been developed.

1) User is approached and forced to start the authentication process
2) User provides sample to *Sensor*
3) Sensor data is processed to *Feature Extractor*
4) Extracted features are send to *Matcher*
5) Matcher uses *Template Database* to create score.
6) Score is sent *Decision Maker*
7) Access is either granted or refused.

This indicates that the only threat vector for coercion is at the sample provision stage. However, this does not mean that the only place for coercion detection is based around the sensor area. This would depend on the biometric - coercion fusion of the system. For example, coercion detection could be deployed at the sensor level however as there is no analysis of the sample until the feature extractor process the coercion techniques would be based here. However if a techniques such as Intentional False Authentication is used, then there could be a sub-module within the sample collection process which identifies what sample has been provided. This would not extract features for the security process. Instead it would simple look for an intentional false authentication data provision. This can be seen within Figure 2.

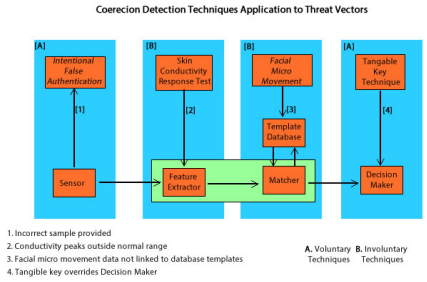

Fig. 2: Coercion detection techniques application to threat vectors

As Figure 2 shows while the main threat vector is at the sensor level and can be dealt with by a IFA technique, different types of coercion detection techniques can apply throughout the authentication process such as TKT at the decision making stage. There are obvious factors that need to be considered when creating coercion detection techniques such as user intimidation, forgetfulness or poor knowledge. Therefore to minimise this issue other techniques of coercion detection are considered, however, to do this the different types of coercion detection techniques were considered and proposed.These factors underline some of the basic concepts within coercion and the current thinking is to split techniques by their individual requirements, in much the same way liveness detection characteristics are considered. For coercion, this means that they are categorised as either involuntary, voluntary or environmental.

1) Involuntary Techniques: Involuntary techniques cover a large range of factors using physiological signals provided by the user's auto-response to specific stimuli. Coercion detections physiological signals would correspond to emotional outputs such as fear, stress and so on. Therefore deviation from a predefined median level would denote active coercion and the system could act accordingly. There are a variety of emotions that could be used to denote coercion such as stress, fear, disgust and so on. There has been great success gathering data based on these emotions as shown by [13] and [14] utilising skin conductivity response tests.

However, there are some disadvantages associated with this technique when specifically using stress as an indicator of coercion. This is due to the ubiquity of stress within the modern workplace environment; therefore it can be claimed that it would not necessarily denote coercion, instead it would be caused by a host of other factors such as exercise, tension, work related stress etc. Therefore,stress's suitability as a coercion indicator [15] would be questionable.

These affect feedback techniques have been studied for many years, primarily within the HCI and machine learning areas as identified by [16]. One universal problem with these physiological data capture techniques is that there is a range of noise factors that can cause the data to peak and trough. Without techniques such as this, noise can have a huge effect on coercion detection. One such example uses blood pressure levels to detection coercion. Elevated blood pressure can be caused by fear, and subsequently can be used to denote coercion, by taking advantage of the fight or flight reflex discussed by [17] and iterated upon for the subsequent Cannon-Bard Theory [18]. The main question here is how can this data be differentiated from simple blood pressure elevation caused by medical noise or physical exertion. Therefore, when developing with these techniques and consideration, the onus must be put on technique and its capabilities to identify relevant data. This noise data is very important and adequate noise cancellation techniques must be developed to produce accurate results, however this is not within the scope of this paper.

The key factor to consider with involuntary techniques is that the technique do not rely on the user knowingly providing coercion data. Therefore the fusion capabilities of the technique can be greater than with involuntary techniques, additionally the subtly of the technique will also be much greater potentially making the process safer for users. However there are a plethora of ethical, legal and social factors to consider with automated sample gathering techniques.

2) Voluntary Techniques: While most coercion techniques revolve around the automatic gathering of physiological data; voluntary techniques focus more on the user providing data to the system that it can then use to denote coercion. These techniques are voluntary approaches because they rely on the user to provide data of some kind, and while it can be argued that medical techniques are also voluntary, the distinction is

that there is an additional conscious process, by the user, to provide a sample. This is normally done with non-medical data, for example, speaking a password or selecting a pattern.

There is a variety of forms this could take, for example, the user may carry a key that may be used as a 'panic alarm'. A second approach would be to utilise a selection of passcodes/keys, that do not correspond to the correct authentication pass-code, instead they would be there to specifically denote coercion. Although to be thoroughly effective the technique would have to be completely integrated within the full biometric system. Otherwise the use of the traditional key system would be seen as a simple and easier approach to security. Without the thorough integration, it would also become obvious to the attacker that some preventative measure was being taken as the inclusion of a key in the final stage would become suspicious and therefore reduce the effectiveness of the technique.

This highlights one of the main problems with voluntary techniques; the user is responsible for the data submission. This can lead to problems occurring including users being unable to provide the data, providing incorrect data due or even a lack of subtlety when providing the sample. This subtlety factor becomes very important when considering different techniques of data submission. If a technique is subtly and easy to present then it is harder for the attacker to detect the subterfuge.

3) Environmental Techniques: Whilst the other techniques focus on the user as a data provider, environmental techniques instead utilises the environment as an indicator of coercion. This technique can be problematic to implement as it does not focus on the different variants of the user, instead it correlates data regarding the user as a focus point. For example the use of cameras and proximity maps can depict if there are people close together. Whilst on its own this does not denote coercion, when combined with appropriate security protocols the technique can become more impressive. For example, all users must make sure they are standing on their own when authenticating into a system, no more than one user next to a biometric scanner at any one time etc. Therefore, if a proximity sensor is able to detect multiple people closer together then it can indicate coercion.

Obviously there is a host of potential problems with this form of approach, least of all the ease of misunderstanding. Using the above example, if two users were carrying a heavy parcel, they would be identified as coercion and therefore the system would respond, in this case erroneously. There are also other noise based concerns, such as how other data sets impact the system, can humans be identified specifically or will other species cause a false rejection, will other heat signatures set of proximity response and if so how can this be dealt with. These false reject samples would create a generally untenable system and it is for this reason that most environmental techniques have been dismissed in this research.

For these reasons it might be practical to use environmental techniques as a secondary authentication, especially if coercion fusion is being considered. By using an affect technique as the primary data collection tool and an environmental technique as the secondary scanner. This would improve the overall security, and would allow the system to more easily deal with coercion, however it would also add complexity, time of scans and overall efficiency. This coercion fusion is something that merits further research bu has not been covered in this paper.

These techniques show the styles of coercion detection that can be developed. However to properly develop coercion detection techniques an understanding of what underlying characteristics are required. Therefore the next section will cover the salient characteristics pertinent to coercion detection.

IV. Development

While the discussion and development of actual techniques are very important, there is a plethora of other concerns such as the identification of the underlying principles relevant to the development and implementation of coercion techniques. The following highlight the main factors to consider when developing a coercion detection technique.

A. Performance

Due to the potential variety of coercion detection, the performance of the individual methods can differ dramatically depending on the type and effect of said technique. For example, a tangible 'panic key' can have a high-performance measurement as they are easy to use, cheap to manufacture and already quite ubiquitous in society however they can be easily circumvented. Alternatively, techniques using affect data are much harder to quantify due to the range of divergences. This is primarily due to the lack of available data on coercion techniques and the emphasis of physiological testing in social sciences instead of computer science. Most of this research, into stress and fear detection, has been conducted in other areas such as [14]s work based around poker, and while the focus is different to coercion detection, the premise postulated therein can still be applied due to the underlying non-specificity. For example, this particular work identifies that detecting stress and lying only achieved an 82% and 71% success rate, which would provide a very poor degree of security, however this figure would have to be taken into account considering the age of the research, the subject area it is being considered in and the specific techniques of data collection as another research has had markedly superior results such as the 90% success rate within [16]s work. Another flaw, for direct security use is that this many technique require long periods of data collection, such as [14]'s work where testers would have data collected about them for an extended period (approximately 15 minutes) which would not be viable within coercion detection, as like biometric security and liveness detection the speed in which the sample is gathered and process is of utmost importance.

While these techniques could be utilised in a variety of situations, the exact implementation would be colossally ineffective due to the time was taken to gather samples. Therefore, any techniques would have to be suitably adapted to the needs of coercion detection and the specific environment being designed for. The main point of these distinctions is to show that the effectiveness of a technique is not limited just to the current lack of techniques. Instead it is only limited by an overall lack of research and understanding of the scenarios it is being utilised in. Therefore to identify performance, the main factors to consider would be the speed of data collection, the accuracy of data collected and ease of implementation.

B. Heterogeneity

Heterogeneity, while often focusing on devices, is a factor that can have far reaching implications throughout the development of systems. Within coercion detection, the heterogeneity of techniques can also be considered as the specificity level. This details the ease in which the techniques can be incorporated across multiple scenarios, techniques and devices. Therefore, it must be identified, as thoroughly as possible, what techniques are most relevant and which are best suited to individual implementation.

As coercion detection is an extension of biometric security the comparative link between security, liveness and coercion must also be considered and this tri-modal will identify what is most relevant within the situation. A lack of heterogeneity here will cause numerous problems to occur such as lack of efficiency. These factors lead to the following assumption that the most effective techniques will be those that can be used throughout the different levels of biometric security. Therefore, creating a thoroughly integrated multi-modal, and multi-security system.

C. Fusion

Fusion details how the techniques will work within the overall biometric environment. How will it integrate with the basic security process as well as the liveness process. When dealing with fusion, the main focus is to combine different techniques, from whatever stage of the security process they are at, in the most efficient and effective way possible. This is normally done within each section, for example, a multi-modal biometric system would contain iris and facial recognition to improve the overall degree of security, within liveness detection blood pressure and skin conductivity tests may be undertaken. While this is the normal route, there is also the additional concept of multi-layer fusion.

As well as the initial fusion between coercion techniques, layered fusion would have to be considered within multi-modal systems. Fusion that would contend with security, liveness, and coercion methods would have to consider the relevant techniques in more detail, as while one technique may be acceptable for a security and liveness environment, the incorporation of coercion may turn the technique into an ineffective style. For example [13] identifies that when utilising multi-modal vocal and emotive systems the effectiveness drops with emotive speech, therefore showing that fusion does not necessarily mean automatic improvement. Alongside this would be specific extra problems, as the emotive aspects would be utilised as an integral part of coercion detection due to the emotional undertones of the subject, therefore degrading the technique even further. This exemplifies the necessity to make sure that the techniques used are the most applicable, and while this is very difficult to do currently due to the lack of techniques and the poor categorisation system.

D. Cultural implication

Unlike many areas of computer science, the effect of culture within the subject is minimal or non-existent, coercion detection has some definite cultural implications. These occur due to the innate individuality of coercion detecting techniques, and it is not just cultural but individual implications that can dramatically effect the way coercion detecting techniques work. For example, certain cultures may find specific techniques distasteful and, therefore, there would be an unwillingness to accept their integration into systems [19]. While there are minimal technical factors that would effect this the cultural implication could have wide-ranging effects and therefore, the user acceptance would be required to complete a final implementation.

E. Medical Implications

Medical data comprises the main bulk of biometric detection samples, therefore, demanding constant reinforcement of validity, permanence, etc. These factors can be dramatically affected by medical intra-variance due to the transient nature of physiological based data. These effects can dramatically change a collected sample to such a degree that they would classify as being coerced even when they are not, completely due to the medical noise factors. For example, a user that is being coerced may have an elevated blood pressure due to the physiological, and psychological, stimuli identified in the fight and flight reflex postulated by [17] and discussed in countless works such as [20].Alternatively, the user could have jogged to work similarly elevating their blood pressure. While this concept is overly simplified the premise holds true throughout the technique.

Therefore, it is imperative that different techniques are assessed on the relevant susceptibility to medical factors which is especially important when considering any fusion plans. This is because the combinations of similar techniques for both liveness and coercion, while potentially efficient, would provide a large target for nefarious user's spoof attacks based on medical data. Additionally, if the same characteristic for liveness and coercion detection is being used as a standard, then they are even more so susceptible to medical noise that affects the singular data type, for example, blood pressure deviations.

F. User Acceptance

A traditional problem with new technology and especially biometric systems is the user acceptance of the technology [21] [22]. While users can sometimes be reluctant to adopt new technology, for a variety of reasons, including age, background, opinion, etc. [23]. As [8] identifies biometric samples deriving from data that is often very personal to a user, data that is rarely called upon for any other reason, except for medical situations, immediately providing cause for potential consternation. For example, the taking of fingerprints may well have criminal connotations for users due to the technology's ubiquity within law enforcement scenarios. Liveness samples may include blood pressure monitors that obviously have some definitive health connotations, including the user's unwillingness to accept medical information, because of embarrassment or fear, etc. The same features can also have the same problems for coercion detection. Therefore, when implementations occur, sufficient consideration must be given to the acceptance of the technology, because if a user does not wish to use the device/technique then, it would be difficult to expand in.

This reluctance would cause a host of issues for most biometric, liveness and coercion techniques as the primary

form of the sample would be more difficult to identify and utilise, making voluntary techniques exceedingly difficult to implement. Secondly biometric systems have had a very bad press within the media and there are numerous occasions where biometric systems have been spoofed due to the loss of or theft of a sample, both within real environments, and a host of popular cultural formats. While these opinions are often erroneous, due to the elaboration of the media, the poor public opinion has sustained and, therefore, further alienates users. This problem is one of the most difficult to address as it deals with changing the opinions of users, something that traditionally is very difficult. To achieve this there are many different techniques including a thorough education process, identifying that biometric environments are as safe, and not as portrayed within popular media alongside a progressive and systematic inclusion of the technology within popular mediums. For example, the inclusion of biometric security options within smart devices will allow the users to become familiar with the technology and hopefully more accepting of different security methods in general.

G. Noise

Many of the factors that are relevant for noise within biometric and liveness detection will also be relevant for coercion. However, there are some subtle differences as coercion is not authenticating or verifying a user. Simply identifying if the user is being coerced or not. Therefore, while the effect of noise is important, it will not have the same degree of impact as it does within the initial biometric security process. While it may not have the same degree of importance as biometric security it is still needed so that the exact effect noise has on coercion detection is understood. The traditional understanding is that noise provides extra data that detracts from the overall sample, therefore making it harder to gather specific features.

As most coercion detection techniques are based around medical data and it has been shown that medical noise can exist from a variety of sources such as exertion, medical condition, etc. This noise will make the sample deviate somewhat from the expected range, therefore potentially preventing coercion acceptance. One theory could include the integration of robust coercion detection algorithms that attempt to remove any noise that occurs. The identification of what form the noise data takes is something that must be considered. Is the noise medical in nature as discussed earlier, if so what are the potential proofs against it and how can it be dealt with? Are other factors, such as environmental, changing the sample enough to impact the authentication process and if so how susceptible is the technique to these factors? These factors must be taken into account when constructing coercion detection techniques as without these factors being addressed the more chance that a security threat will occur and if this threat can exist then the overall effectiveness of the system will be reduced accordingly.

The sub areas have identified th salient factors a coercion detection technique must have, therefore the following section will highlight some of the techniques developed.

V. Novel Techniques

As mentioned one of the major flaws of coercion detection is the lack of techniques. The following four techniques cover both voluntary and involuntary styles, and as Figure 2 shows these technique can be used within different areas of the biometric process, even though they are gathered around the sample provision threat vector.

1) Tangible Key Technique: The first technique to be considered is Tangible Key Technique (TKT) which revolves around the use of a specific piece of hardware or software that is tangible (in its base form, or requiring additional hardware such as a phone in the case of an application). The main advantage of this technique is that the device is heterogeneous and, therefore, it does not discriminate against users, subsequently, it can be used within across almost any technique. For example a fingerprint sample cannot function if the user does not have fingers that would cause collectability problems as well as discriminating against the user. However a TKT does not have these problems as the device can be easily developed to take into account the specific issues it faces. However there are some issues surrounding these devices: for example if a technique uses tangible media then it can be stolen, lost or damaged, an app can be corrupted or the medium it is installed on can be stolen, damaged, etc. [24]. It also relies on the user to make sure they always carry the device, something less of an issue when considering an app, but still an important contribution. Therefore, it would be best if the device was small enough to be easily transportable.

This technique would work within the decision stage of the biometric process, as it would be able to overrule the sample being collected. IF this technique was used and the technique has been activated, then the sample provided would be ignored instead the TKT would indicate that a refusal should occur within the decision maker, therefore disallowing the attacker access.

2) Skin Conductivity Response Tests: Skin conductivity response signs can change when subject to strong emotions. The physiological signs of these emotions provide the information that is needed to detect the state of a user, in the case of coercion detection, these emotions would focus on negative ones such as fear and disgust[25] [26]. This technique requires additional hardware and is prone to user noise such as the effects of cosmetic, skin-care products and medical factors that can change the test including medication ingestion and generic medical variations [27]. The main advantage of this technique is that it has the potential to be very accurate and can be used easily within a fusion based system, due to its use within liveness and initial sample collection techniques. However, this technique has one caveat as it is dependent on background research and while this physiological testing has been considered for some years the application within coercion detection is very new and, therefore, it would be necessary to take every caution when integrating the technique.

This technique would work within the feature extractor stage of the biometric process. Whilst the biometric data is being gathered and features being extracted, the skin conductivity response test would also have its features extracted and it would then be checked against the data range denote coercion. If it is outside this range then it will return a negative access response to the decision maker.

3) Intentional False Authentication: Intentional False Authentication (IFA) checks if a user is being coerced by allowing

them to provide a sample that is deliberately incorrect. For example instead of using the index finger to authenticate the user will use a designated different finger or the thumb and when this is detected the system automatically knows that the users are being coerced. The main advantages of this technique are that it can be applied to almost all other biometric and liveness techniques, as the user has merely to designate a separate authentication sample to be registered as the coercion measure. This can be done by the user or by the system and has some advantages, for example, there is a limited need for additional hardware as the sample being used is from the same type and the heterogeneity it affords is excellent as most samples will have an easily identified alternative. One major flaw with this technique is that it relies on the user more than others. Normally the user has to provide a sample to authenticate into the system. However this technique would also require them to not only remember what their false sample is, but also be able to provide it without the attacker noticing. This not only adds the issue of user subtlety but also could potentially provoke the attacker if discovered, both of which need to be minimised.

This technique would work within the sensor stage of the biometric process. Whilst the biometric data is being gathered the user would provide a false sample, different fingerprint etc, which would stop cause a failure to occur when matching to the fingerprint database, or within the sensor itself, depending on the style of biometric.

4) Facial Micro-Movement: Facial Micro-Movement (FMM), which is based on FACs [28], is a novel technique that is based around the detection of emotion and the corresponding physiological characteristics therein. Within coercion detection, the obvious focus is on negative emotions and ones that can be associated with coercion detection, mainly fear, anger, distress, etc. This technique is based on the FACS which has been used within the affect testing area for some years and has been identified as the superior technique in the area [28] [29] due to the higher accuracy and ease of use. The main advantage of FMM is that it is very heterogeneous as there is minimal additional hardware needed and only some additional software to help decipher the AU (action units) that make up the data collection process. However while the technique works well with facial based techniques it obviously has no connection to other styles therefore potentially limiting its usefulness. One other issue to contend with is that FACs is often different depending on who has coded the system, as there is a degree of change from coder to coder. It is imperative that all use of this techniques follow the same coding pattens to enable good testing and analysis to occur.

This technique would work within the sensor stage of the biometric process. As the FACs would be able to denote if the user is being coerced by identifying the AUs denoting fear, anger etc. This would then be compared with templates within the template database and an appropriate response could be made.

VI. Conclusion

This paper identifies the appropriate coercion threat vectors, and highlights that sample provision is the primary threat. Then a number of techniques have been identified, along with underlying characteristics that would allow coercion detection to occur. The key factor to continue is to highlight the individual techniques and create experimental tests to check for suitability and applicability. Currently a TGK is a good method of coercion detection, but has some innate problems such as ease of loss and counterfeiting. Whereas a IFA theoretically can be very accurate, but relies heavily on the acceptance and reliability of the user. These factors need to be correlated and classified, ideally within a taxonomy which would enable researchers and users to better understanding their strengths and weaknesses.

References

[1] "Theft Act 1968," pp. 1–12, 1968. [Online]. Available: http://www.legislation.gov.uk/ukpga/1968/60

[2] J. Flatley, "Crime in England and Wales, Year Ending March 2014," *Office for National Statistics*, 2014. [Online]. Available: http://www.ons.gov.uk/ons/dcp171778_371127.pdf

[3] A. S. Network, "Aviation Safety Network ¿ Statistics ¿ By period ¿ airliner hijackings." [Online]. Available: http://aviation-safety.net/statistics/period/stats.php?cat=H2

[4] Interpol, "Maritime piracy / Maritime piracy / Crime areas / Internet / ... Maritime piracy," p. 2013, 2015. [Online]. Available: http://www.interpol.int/Crime-areas/Maritime-piracy/Maritime-piracy

[5] J. L. Wayman, "Technical testing and evaluation of biometric identification devices," in *in Biometrics: Personal Identification in Networked Society, eds. A. Jain et al. (Kluwer Academic Press*. Springer US, 1998, p. 345.

[6] N. Bartlow and B. Cukic, "The vulnerabilities of biometric systems an integrated look and old and new ideas," West Virginia University, West Virginia University, Tech. Rep., 2005.

[7] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, 2007.

[8] K. Nandakumar, Y. Chen, S. Dass, and A. Jain, "No Title," *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, vol. 30, no. 2, 2008.

[9] T. van der Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," in *Smart card research and advanced applications: IFIP TC8/WG8. 8 Fourth Working Conference on Smart Card Research and Advanced Applications, September 20-22, 2000, Bristol, United Kingdom*, vol. 31, no. 0. Kluwer Academic Publisher, 2000, p. 16. [Online]. Available: http://books.google.com/books?hl=en&lr=&id=mGOnonNnr7AC&oi=

[10] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of Artificial "Gummy" Fingers on Fingerprint Systems," in *Proceedings of SPIE*, vol. 4677, no. 1, 2002, pp. 275–289. [Online]. Available: http://cryptome.org/gummy.htm

[11] O. E. Dictionairies, "Definition of coerce in English:," 2014. [Online]. Available: http://www.oxforddictionaries.com/definition/english/coerce

[12] R. Williams and A. Systems, "BAE Systems Autonomous Capability Overview Introduction & Agenda," pp. 1–21, 2014. [Online]. Available: http://www.stfc.ac.uk/resources/pdf/richardwilliams.pdf

[13] J. Healey and R. Picard, "SmartCar: detecting driver stress," in *Proceedings 15th International Conference on Pattern Recognition. ICPR-2000*, vol. 4. Barcelona: 2000. Proceedings. 15th International Conference on Pattern Recognition, 2000, pp. 218–221.

[14] M. Sung and A. Pentland, "PokerMetrics: Stress and Lie Detection through Non-Invasive Physiological Sensing," 2005. [Online]. Available: http://citeseer.uark.edu:8080/citeseerx/showciting jsessionid=5DB10DCA426C12D7434B594288FD67E8?doi=10.1.1.153.9203&sort=asc

[15] S. Bethune and J. Panlener, "Stress a major health problem in the U.S., warns APA." 2007. [Online]. Available: http://www.apa.org/news/press/releases/2007/10/stress.aspx

[16] M. a. Sayette, J. F. Cohn, J. M. Wertz, M. a. Perrott, and D. J. Parrott, "A psychometric evaluation of the facial action coding system for assessing spontaneous expression," *Journal of Nonverbal Behavior*, vol. 25, no. 3, pp. 167–185, 2001.

[17] J. R. Angell, *Bodily Changes in Pain, Hunger, Fear and Rage; An Account of Recent Researches into the Function of Emotional Excitement*. New York and London: D. Appleton and Co., 1915, vol. 42, no. 1089.

[18] S. Rathus, *Psychology: Concepts and Connections*. Belmont: Wadsmorth, 2012.

[19] R. W. Picard, E. Vyzas, and J. Healey, "Toward machine emotional intelligence: Analysis of affective physiological state," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 10, pp. 1175–1191, 2001.

[20] J. Etherton, M. Lawson, and R. Graham, "Individual and gender differences in subjective and objective indices of pain: Gender, fear of pain, pain catastrophizing and cardiovascular reactivity," *Applied Psychophysiology Biofeedback*, vol. 39, no. 2, pp. 89–97, 2014.

[21] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems fir Vudei Technology*, vol. 14, no. 1, pp. 1–29, 2004.

[22] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, J. L. Wayman, and A. Hong, "Biometrics: A Grand Challenge," in *Proc. International Conference on Pattern Recognition (ICPR) VOL ii*, Cambridge, 2004, pp. 935–942.

[23] W. Elgarah and N. Falaleeva, "Adoption of Biometric Technology: Information Privacy in TAM," in *AMCIS 2005 Proceedings*. AMCIS 2005 Proceedings., 2005, p. Paper 222. [Online]. Available: http://aisel.aisnet.org/amcis2005/222

[24] W. Stallings and L. Brown, *Computer Security: Principles and Practice*. Prentice Hall, 2012.

[25] P. Gupta and D. Gao, "Fighting Coercion Attacks in Key Generation using Skin Conductance," in *Proceedings of the 19th USENIX Security Symposim (USENIX Security '10)*. CA: USENIX Security'10 Proceedings of the 19th USENIX conference on Security, 2010, pp. 469–484.

[26] K. Tabbert, R. Stark, P. Kirsch, and D. Vaitl, "Dissociation of neural responses and skin conductance reactions during fear conditioning with and without awareness of stimulus contingencies," *NeuroImage*, vol. 32, no. 2, pp. 761–770, 2006.

[27] R. Edelberg and N. R. Burch, "Skin resistance and galvanic skin response. Influence of surface variables, and methodological implications." *Archives of general psychiatry*, vol. 7, no. 3, pp. 163–169, 1962.

[28] P. Ekman and W. V. Friesen, *The Facial Action Coding System.* Palo Alto: Consulting Psycological Press, 1978.

[29] C. E. Izard, *The maximally discriminative affect coding system (MAX)*. Newark: University of Delaware, Instructional Resource Center, 1979.