A Cyber-Physical Approach to Trustworthy Operation of Health Monitoring Systems

Krishna K. Venkatasubramanian[1], Ayan Banerjee[2], Sandeep K.S. Gupta[2], and Robert J. Walls[1]
[1] Worcester Polytechnic Institute, and [2] Arizona State University

***Abstract*—Continuous health monitoring system (CHMS) are a collection of networked sensing devices that continuously monitor a user who is carrying them. The sensors can be worn by the user (e.g., fitbit or jawbone) or be part of a device that user carries (e.g., smartphones). Trustworthy operation is essential for CHMS due to the sensitive nature of the information they collect and the wireless transmission of the data to a sink/base-station entity for transport to a medical cloud for long term storage in a patient health record (PHR). In this regard, in the past we have proposed a scheme known as Physiological signal-based Key Agreement (PKA) to enable plug-n-play (i.e., transparent to the user in terms of configuration or setup) information security between wearable sensors that had access to same physiological signals (e.g., ECG, PPG). In this paper, we present Physiology-based System-wide Information Security (PySIS), which uses the concept of generative models (which generate synthetic physiological signals for a user) to extend PKA to enable end-to-end information security in CHMS from the sensors to the PHR. The crucial difference is that now we do not need to have access to the same physiological signals at both ends for our protocol to work. In addition, if PySIS fails and data leakage occurs in the system, we also propose a logging mechanism to perform forensic analysis of the system.**

I. Introduction

Smartphone-based health monitoring and the emerging field of wearable systems have demonstrated great potential in a broad range of applications in healthcare and wellbeing. These systems utilize an array of lightweight sensing devices that collect and wirelessly transmit data to a sink/base-station entity for eventual transport to a medical cloud for long term storage in a patient health records (PHR). Examples of applications of *continuous health monitoring systems* (CHMS) include physical activity monitoring, emergency response, and rehabilitation. These systems intend to improve health outcomes, decrease isolation, reduce health disparities, and substantially reduce costs have the potential to produce annual cost savings of up to $81billion$ to the healthcare expenditure [1].

In this paper, we consider that trustworthy operation of CHMS includes two aspects: a) data security in CHMS, which ensures that there is no data leakage leading to effects such as privacy violation or other malicious actions, and b) even if there is data leakage the CHMS can always detect such an event and take actions.

Recent years have brought increased attention to information security vulnerabilities in medical devices and sensing elements [2]–[4] that manifest due to lack of secure communication between the devices and entities that manage them (i.e., data sinks/programmers). Lack of security in CHMS not only harms patient privacy, but may also physically harm the user (i.e., the host). Adversaries can introduce bogus data, modify/suppress legitimate health data — inducing erroneous evaluation of a person's health, untimely administration of treatment, or denial of service (DoS) — on an unsecured CHMS. The issues of security for CHMS can be addressed from many perspectives, for instance, much work needs to be done to improve the quality of software being run on these devices and the way regulators ensure that the system is secure [5]. However, in our efforts we are focused on ensuring *information security*, that is, the data the CHMS generate and communicate are accurate and not tampered with. This has two elements:

- *Data Collection Security:* This is essentially about securing the CHMS data collection infrastructure. Ensuring data collection safety therefore requires ensuring that the medical data is not tampered with or observed by authorized entities as it transits from the sensors (that generate them) all the way to the PHR. Traditional solutions for data collection security have considerable initialization and management costs, especially those related to the deployment of cryptographic primitives (e.g., key distribution, rekeying, and tamper-resistance). These approaches assume a large degree of control in terms of deployment [6]. Hence, they require a hospital or home environment for implementation. As the general acceptance of CHMS and the number of constituent devices increase, maintaining the same level of deployment control may not be feasible. Consequently, in order to minimize the cognitive load on the *users* – both CHMS hosts and caregivers – the CHMS have to be considerably easy to use. This is especially true for security solutions, which if cumbersome can simply be ignored.
- *Data Reconciliation Security:* Given the ever increasing number of monitoring devices on a patient from specifically designed wearable devices of a BAN to a smartphone based sensor data, the number of personal health records (PHRs) maintained for a user is also ever increasing. The PHRs are typically maintained by the monitoring system developers and are usually isolated and independent of each other. For this data to be useful for the user, it is important for the data to be reconciled (aggregated) in one place. Much like apps like MINT [7] reconcile a person's financial data in one place. This process of reconciliation has to be done in a manner that is secure. This means that medical data leave the PHRs only if an authorized party requests it and the data protected during transit. One could imagine a system where the

This work has been partly funded by CNS grant # 1218505, IIS grant # 1116385, and NIH grant # EB019202. Email: kven@wpi.edu, abanerj3@asu.edu, sandeep.gupta@asu.edu, rjwalls@wpi.edu

PHRs use passwords for authorizing users. An aggregator therefore establishes an SSL connection with the various PHRs and uses a username and password over the secure link obtaining the data. Given the diversity of apps that collect health data from a user, the number of passwords that the user has to remember will be much higher and therefore tedious compared to other types of information such as financial data.

Figure I illustrate the data collection and reconciliation process. Our aim is to make sure the authorization and the data exchange happens during data collection and reconciliation in a CHMS without the user being actively involved. In this regard, we propose a unified approach to collection and reconciliation problem — one that takes the cyber-physical character of CHMS enabling security. Cyber-physical security solutions (CyPSec) has been proposed as an alternative to traditional information security approaches (e.g., PKI and passwords) for medical monitoring systems such as BANs [8]. CyPSec solutions use the environment of the operation of the system, in this case the human body, to derive or facilitate the exchange of essential security primitives (e.g., cryptographic keys) that will enable information security within the system. Moreover, as with any security solutions PySIS can also be compromised given an adversary who has the required resources. In case PySIS is compromised, the CHMS should also have mechanisms to perform forensic analysis to pin point, which sensor or, which communication step was compromised or at the least detect an attack from an adversary.

In this paper, we present a unified CyPSec-based information security solution called **Physiology-based System-wide Information Security (PySIS)** for CHMS that secures both the data collection and reconciling with one general approach using (1) an authentication key agreement process based on physiological signal features for hiding and unhiding, and (2) physiological generative models which produce synthetic clinically-relevant physiological signals based on an analytical model trained using physiological signal statistics collected from the user. The main idea is to use features derived from the user's actual physiological signals to hide a cryptographic key and use features derived from synthetic physiological signals using appropriately user-specific physiological generative models to unhide this key. The successful unhiding of the key provides two advantages for the entities that have access to the user's physiological data or generative models, it provides: (1) *authentication* based on the shared knowledge of user's physiological signal features, and (2) *confidentiality and data integrity* through the subsequent use of the cryptographic key exchanged. Further, the PySIS does not even require the two communication entities to have access to the same physiological signals or their generative models. In fact PySIS works with both coherent and incoherent signals. *Coherent signals* are generated from the same basic physiological process, e.g., electrocardiogram (ECG) and photoplethysmogram (PPG) obtained from the beating of the heart.While *incoherent signals* are generated from different physiological processes such as electroencephalogram obtained from the brain's electromagnetic activity, and ECG obtained from heart beats. Finally, PySIS make security plug-n-play, largely transparent to the users and therefore easy to deploy and use.

For forensic analysis of the CHMS, we propose *investigator-driven* approaches for forensic analysis of system failures; whether those failures are the result of benign circumstances or malicious attack. At the core of our approach is a tamper-evident logging system that faithfully records system events—even when the logger itself cannot be trusted. We also explore the dichotomy inherent in collecting data without knowing what information will be relevant *a priori* and quickly pinpointing the source of the attack or failure. To address this challenge, we use data provenance and semi-automated analysis to infer and prioritize the data most relevant to the current investigation. Our forensic logging relies, in part, on an extension of the tamper-evident semantics developed in [9] and others [10], [11]. While these works form a strong foundation for the research efforts described in this proposal, they do not address many of the key challenges of forensic analysis. In particular, tamper-evidence is a necessary component to forensic analysis, but these semantics do not help the investigator analyze the attack itself [12].

Before we delve any further into PySIS we present some background on how physiological features can be used for secure key hiding/unhiding (i.e., key agreement) and how generative models work.

II. Background

Here we present a quick summary of the two principal components of PySIS namely, physiological-feature-based key agreement (PKA) and physiological generative models.

A. Physiological-feature-based Key Agreement (PKA)

The variability in the human physiology can be used to derive fresh symmetric cryptographic keys for secure communication between any wearable device with access to the same physiological signals [6]. Entities capable of sensing the same physiological signal can use common physiological signatures to hide and un-hide a secret key. In this protocol, the sender generates a random key and hides it using frequency-domain features generated from recently measured physiological signals obtained from a person with cryptographic construct called the *fuzzy vault* [6]. The vault is then transferred to the other receiver, which then uses its own frequency-domain features generated from measured or generated physiological data to un-hide the random key.

The key hiding using physiological features is a lightweight signal processing process that executes at the sender. The sender senses physiological signals for a given time, e.g., 30 seconds, and performs a windowed 256-point FFT on the signal snippet. The sensor then runs a peak detection algorithm on the FFT and derives peak indexes and peak values, which are concatenated to form a 16-bit feature. The sender then generates a random 128-bit key and splits it into $n + 1$ coefficients of a nth order polynomial. The features are then transformed using the polynomial to form a set of ordered pairs (x, y) of feature values and their polynomial evaluations. This set is then obfuscated with random pairs (x', y') called *chaff points*, such that y' is not the polynomial evaluation of x'. The ordered and the chaff points together form the *fuzzy vault*. This vault is then sent to the receiver, which has its own set of 16-bit features generated from concurrently measured physiological

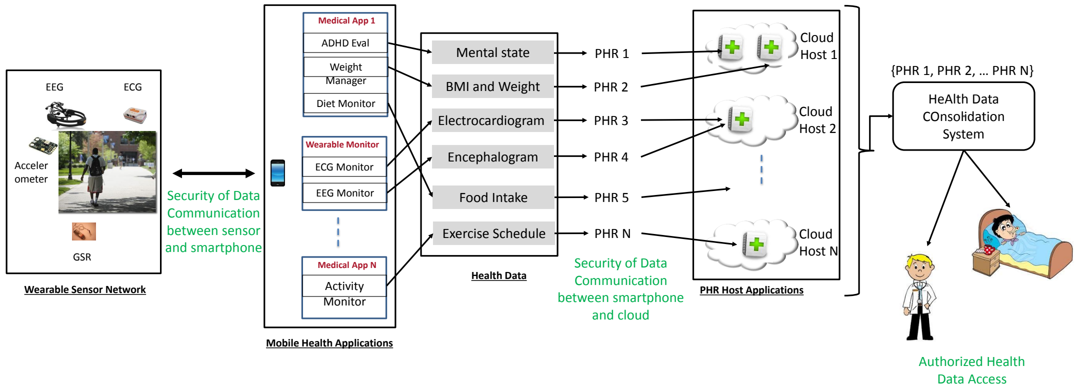

Fig. 1. System Model for Health Data Collection and Reconciliation

signals. As long as the receiver has more than $n+1$ features in common with the sender, it can use Lagrangian interpolation to reconstruct the polynomial and obtain the secret key from its coefficients. As long as the number of common physiological features between the sender and the receiver is greater than n, where n is the order of polynomial used, the receiver will successfully deriving the secret key from the vault. However, if this vault is received by an attacker who does not have access to patient data, it has to go through all possible combination of $n+1$ points out of total number of points in the vault which is combinatorial in order. For example of 9th order polynomial and 4000-point vault, the complexity for the attacker to break the vault is equivalent to brute-forcing a 95-bit key [6].

B. Physiological Generative Models

Generative models of a physiological signal S_A is a mathematical function, which takes personalized temporal and morphological parameters as input and output synthetic physiological signal $\tilde{S_A}$ [13], [14]. The *temporal parameters* (f_A), e.g., heart rate and the standard deviation of the heart rate, change frequently over time. Despite the considerable dynamics of the human body, an important characteristic of human physiology is the periodicity of the waveform of its various physiological signals. The waveform shape within a period is called the *morphology* of the signal and is expressed by the *morphology parameters* (m_A). A generative model is therefore a function $G_A(m_A, f_A, t)$, that when supplied with the correct morphology and temporal parameters generates a diagnostically equivalent synthetic signal $\tilde{S_A}$ for time t. It has been observed that for ECG and PPG signals the morphology parameters change very slowly over the lifetime of a person and hence is a physiological signature [13]. To use a generative model for synthesizing physiological signals the morphology parameters have to be learned from a sample of the actual physiological signal. The temporal properties too have to be obtained from the actual physiological signals, but obviously in real time. Finally, though generative models produce *diagnostically equivalent* signals, the synthesized and actual physiological signals may not match sample for sample. They only match in certain features deemed useful for diagnosis of critical health problems as suggested by a physician.

III. The PySIS principle

The principle behind PySIS is to execute PKA thus enabling authenticated key agreement but replace the raw physiological signals on one end with the diagnostically-equivalent synthetic signals obtained from a trained physiological generative model. Let us consider that the entity A has access to physiological signal S_A and entity B has access to the generative model G_A, and the morphological parameters m_A of the signal S_A. Let us also consider that the entity A was already authenticated to entity B and was sending the most current version of S_A using a secret k_i. The entity A now wants to execute PySIS to renew the key k_i to k_{i+1}. The entity A can generate the new key k_{i+1} and hide it using the vault created by features extracted through the PKA process. The entity B extracts the most recent temporal features f_A from signal S_A and uses the model $G_A(m_A, f_A, t)$ to generate synthetic signal $\tilde{S_A}$. It can then extract PKA features from the synthetic signal and unlock the vault to get the new key k_{i+1}. Our previous work PEES explore this idea in more detail [15]. In this scenario the usage of generative model may seem unnecessary. However, we will see in subsequent sections how we can secure two entities that have access to different types of signal using the same idea. Finally, we will extend this technique to consider automated authenticated reconciliation of PHRs associated with a given person in a transparent manner.

IV. System and Threat Model

At the core of the system is a set of wireless sensors that are either part of a device worn by the user of carried as part of their smartphone. Examples include glucose meters, electrocardiogram (ECG) or photoplethysmogram (PPG), or environmental such as temperature and humidity monitors. Actuating devices such as infusion pumps, can also be used in CHMS however we do not consider them explicitly for this work to keep the discussion simple. PySIS can be easily extended to actuators. The sensors sense physiological as well as environmental signals at a given sampling rate. The goal of the system is to collect data from the sensors and forward them to a medical cloud for storage and caregiver retrieval. The cloud essentially maintains a *personal health record (PHR)* for the user where the data is archived. The transfer of sensor data to the PHR is done usually via a local sink entity called the base station. The base station can be implemented on a variety of devices from generic smartphones to proprietary dongles such as [16] [17].

The data stored in the PHRs may need to be reconciled by the user as needed and we assume the user utilizes an aggregator application for this purpose. The aggregator is assumed to know the location of the various PHRs. Its principal task is to connect over a network with each of the PHR, present the user's credentials and then obtain data. The health data is then available at the aggregator for further analysis as well as access without connecting to the PHR again. We further assume the aggregator and the various PHRs use a common language to communicate with each other such as HL-7 CDA [18] in order to exchange data.

Threat Model: Given the sensitive nature of the data collected by CHMS in their respective PHRs which later need to be accessed, one needs to ensure that the data being exchanged thus is protected from unauthorized access and tampering. In this regard, securing a CHMS requires preventing the adversaries from: (1) joining the network as a legitimate device and introducing bogus health data, (2) accessing confidential health data collected or exchanged while the data goes from the sensors to the PHR and then reconciled from the PHR by the aggregator, and (3) preventing any legitimate health data from being reported or modified during the transit.

V. Physiology-based System-wide Information Security

Let S_A and S_B be the signal features obtained at entities A and B that are trying to use PySIS, then we have two cases to consider: (a) S_A and S_B are coherent that is generated from the same underlying physiological process of the body e.g., electrocardiogram and photoplethysmogram that is related to the cardiac process, and (b) S_A and S_B are non-coherent i.e. generated from totally different physiological process of the body e.g., electrocardiogram from heart and electroencephalogram from brain.

A. PySIS for Data Collection

Data collection requires data to be transferred from the sensor to the PHR via a base station. This means one needs to secure (establish secure communication channel between them through authenticated symmetric key agreement) the various links that exists on this path. Using PySIS, the approach is the same for any pair of entities in the path. We therefore keep our discussion general between two entities A and B on the path. Let us consider that an entity A has access to the generative model of a physiological signal S_A. This means that the entity A has both the morphological parameters m_A and the current temporal parameters f_A of the generative model $G_A(f_A, m_A, t)$ of the signal S_A. A may or may not have the physiological time series signal S_A, however, it has the capability of regenerating a synthetic signal $\tilde{S_A}$ with the generative model G_A which is diagnostically equivalent to the time series S_A. Let us consider that we need entity A to have an authenticated and secure communication channel with another entity B sensing signal S_B having a generative model $G_B(f_B, m_B, t)$ of signal S_B.

Using Coherent Signals: We hypothesize that if two signals are coherent then there will be a considerable amount of correlation among their temporal parameters. This hypothesis has been supported by our previous work where we considered the ECG and the PPG signal and measured the heart rate variability from the two [13], [14]. Although the morphology of the two signals are very different, the temporal properties such as average heart rate, standard deviation etc. reveals very close match among the two signals[1]. Moreover, using the results of our previous work [15], we hypothesize that *the synthetic signal obtained from generative model of a signal, ECG or PPG, has common physiological signature with the original time series of the signals, ECG or PPG respectively.*

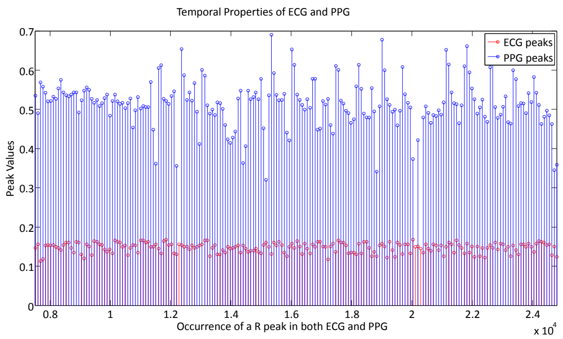

Fig. 2. Temporal parameters derived from ECG and PPG. Results from 24 subjects show high correlation between heart rates derived from ECG and PPG and low error in mean heart rate, standard deviation, and lfhf ratio estimation.

Let the signals S_A and S_B has common temporal parameters f_{AB} as they are coherent. Further let G_A and m_A be the generative model and morphological properties for signal S_A that entity B possess in a pre-deployed fashion.

1) A generates a secret session key k, uses PKA to hide it using frequency-domain features (note these are different from f_{AB}) derived from S_A and send its over to B.
2) B computes f_{AB} from its sensed signal S_B.
3) B then uses m_A and the time domain parameters, f_{AB} obtained from S_B to generate the synthetic signal $\tilde{S_A}$ from its generative model $G_A(f_{AB}, m_A)$.
4) B then derived frequency-domain features from $\tilde{S_A}$ and executes PKA to unhide the key k.

An obvious issue one can raise here is that the entity B needs to posses both the generative model and the morphological parameters of signal S_A. If we need to pre-deploy them, why not pre-deploy actual cryptographic keys. This is true to some extent. However, with PySIS approach we need to redeploy G_A and m_A only once. Any subsequent rekeying will happen automatically. Further, the approach is secure even if the current session key is compromised as a new session key, completely unrelated to the one compromised, can be generated within the system secure. This however cannot be said for key pre-deployment based approaches.

Validation: To validate PySIS for coherent signals we considered 24 subjects form the MIT database [19] that has both ECG and PPG data measured simultaneously. The sampling frequency of ECG was 125 Hz while that of PPG is 60 Hz.

[1] In fact there is some morphological equivalence among the two signals as well, since the position of the R beat of the ECG coincides with the peak of the PPG signal.

We employed a peak detection algorithm to detect R peaks from both the ECG and PPG signals. Figure 2 shows a sample plot of the peaks from both the signals of one subject. There is a very near match in the position of the R peaks. This entails that the temporal properties of may be similar for both the signals. In fact on further analysis we found that the correlation of the heart rate from both the signals is on an average > 0.9 indicating that both the signals have very similar heart rate variability. The difference in heart rate estimation from both the signals was less than 1 beat and the difference in standard deviation estimation was less than 0.8. The fact that the temporal properties are so similar allows us to execute PKA with considerable success.

Using Non-coherent Signals: For non-coherent signals we rely on the hypothesis that *coupling provided by the human body between different physiological processes ensures that some signature of signal S_A is visible on a signal S_B even if S_A and S_B are not produced from the same physiological process*. With non-coherent signals the execution of PySIS is identical to the coherent case, excel the f_{AB} is now derived from a signal S_B that is not coherent with S_A. Experimentation with MIT BIH data [19] shows that there is considerable coupling between ECG signal from the heart with the EEG signal of the brain of an individual. The R peaks from the ECG signal can be obtained from the EEG signal of an individual using complex physiological signal processing algorithms. The time domain parameters of the generative model of the ECG can be derived from these R peaks and can be used in conjunction with the morphology parameters of the ECG to execute PySIS between an EEG sensor and an ECG sensor.

Our approach to extract ECG from EEG signal uses Continuous Wavelet Transform (CWT) [20]. CWT gives information about the available frequencies in the signal at a particular time. CWT uses a basic signal function which is scaled according to the frequency and time shift allowing specific shape properties of the signal to be analyzed. CWT for $x(t)$ signal is expressed as:

$$x(t) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} x(t)\psi^{*}\left(\frac{t-b}{a}\right) dt, \tag{1}$$

where, $a > 0$ is a scaling parameter, b is a shift parameter and ψ is a wavelet function. The scale parameter a, is used to denote how much the wavelet is stretched or compressed. Smaller the value of a, more the compressed wavelet. The shape of wavelet becomes stretched with increase in value of a. For each R-peak in ECG there is a corresponding disturbance in the wavelet transform of EEG signals as shown in Figure 3. The scale 4 [21] parameters from the wavelet transform of the EEG signal exhibit this disturbance with the maximum magnitude.

Validation: With accurate signal processing technique we can extract the time values at which these disturbances occur and hence get the positions of the R peaks in the ECG signals. These temporal parameters can then be used by a generative model to generate a synthetic ECG signal for PKA execution. Simulation results on 10 different patients show a PKA success rate of 20%. Although the success rate is very small, we believe that a more comprehensive signal processing algorithm can ensure better success rate. This is part of our current efforts in this direction.

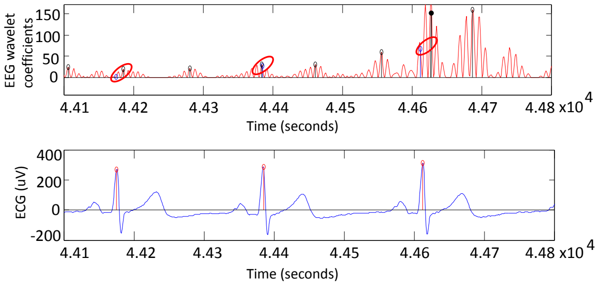

Fig. 3. **R peaks from ECG data and wavelet transform of EEG.**

B. PySIS for PHR Reconciliation

In this era of wearables and smartphones a user has a plethora of non-clinical PHRs recording important information on behavior and physiology that can be useful in managing health risks. Data from the set of PHRs for a given user is very valuable and can be used in two ways: (a) the data can be processed to provide behavioral feedback to the user through smartphone application; and (b) care providers can be granted access to this data as needed during both normal office-visits and during emergencies. Hence reconciliation of these disparate sources of information is an important problem. Traditional techniques for reconciliation of disparate health data are largely manual and requires remembering multiple of username and passwords, at least one for each PHR. This imposes enormous cognitive load on the user given the large number of PHRs that the inevitable ubiquity of sensors and smartphones is bound to create. With an aging population the time when PHR reconciliation is the most useful is the precise time when the user maybe least capable of achieving it, leading to treatment errors and unwanted hospitalization.

PySIS can help in alleviating this problem by enabling automatic, regularly and secure reconciliation of various PHR data by establishing a secure channel using PKA. The idea is to use PHR-based physiological signal time series and generative models on one end and the actual physiological data at the aggregator (user's) end. Assuming one can identify the PHRs associated with a user is known, then PHR reconciliation can be done as follows:

- The aggregator A uses the user's actual physiological signal S_A, derives frequency-domain features from it and uses it to hide a session key and sends it to a PHR (PHR_A) containing user data.
- If PHR_B uses the generative model G_A to generate synthetic signals, derive frequency-domain features and unhide the key.

PHR_B can populate its model G_A using the physiological time-series S_B is has it ins database. If S_A and S_B are the same, the G_A can be easily created using the temporal and morphological characteristics derived from S_B using our approach described in [15]. If the signals and however coherent or non-coherent, then the G_A creation will require m_A being also stored at the PHR_B. This can be done when the PHR is initialized before data collection begins.

VI. Tamper-evident logging system

At the core of our approach is a tamper-evident logging system that records information from all of the devices in the system. Importantly, this log guarantees information will be recorded without modification, even if the logger itself is not trustworthy. At a high-level, our forensic logging system will have the following components: *sensors* which record information in the log; a *logger* sitting on a resource-capable device (e.g., the base station) which collects and stores the records, and *auditors* which use periodic cryptographic challenges to verify the untrusted logger has not tampered with the log. We assume both the logger and any of the clients can be compromised. However, if any auditor remains secure we can detect any tampering.

We use a centralized log to minimize the resource requirements for the sensors and provide a canonical ordering of system events. While we can leverage remote logs to increase data availability and prevent compromises from deleting past logs, using a remote log alone is insufficient as the log must always be available to the system—we cannot assume a connection to a remote server will always be possible. Further, if the base station is compromised, it effectively becomes a malicious man-in-the-middle that can manipulate *all* communication with the remote log, rendering the log ineffective. The forensic logger must record the information sufficient for understanding a *previously unobserved* attack against the system, but the investigator must also be able to locate this relevant information in the deluge of all possible data the system can log.

In a CHMS the relevancy of data depends on the context information. Hence, the investigator driven logger can use the current context information to determine which data is relevant and shows in consistencies with the current context. Since the context is a dynamic variable, the attacker does not have the opportunity to plan ahead and tamper data such that it also agrees with the context information. Hence an investigator driven logger which takes into account the context information to determine anomalies is most likely to be successful.

VII. Conclusions and Future Work

In this paper, we outline a physiological value based system wide security protocol (PySIS). which uses the concept of generative models (which generate synthetic physiological signals for a user) to extend PKA to enable end-to-end information security in CHMS from the sensors to the PHR. Such association can be used to provide information security such as maintaining privacy, authentication, and message integrity during the data collection and reconciliation process within CHMS. An important contribution in this paper is the usage of physiological signal based security between entities with access to different types of physiological signals. In the future, we plan to expand this work to improve the performance of PySIS for non-coherent signals as state above.

While the proposed tamper-evident logging scheme provides a solid foundation for forensic analysis, there other fundamental questions that must be still addressed. (1) How do we provide forensic guarantees in the face of backwards compatibility, allowing unmodified devices to join our system with only a minimal loss of auditing capability? (2) How do we construct and use forensic summaries of the event to identify similar failures in the wearable systems of other patients? Identifying such matches are important to understanding attack trends across the entire population.

References

[1] R. Hillestad, J. Bigelow, and et al., "Can electronic medical record systems transform health care? potential health benefits, savings, and costs," *Health Affairs*, vol. 24, no. 5, pp. 1103–1117, 2005.

[2] D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W.H. Maisel, "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses," in *IEEE Symposium on Security and Privacy*, may 2008, pp. 129–142.

[3] C. Li, A. Raghunathan, and N. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*, 2011, pp. 150–156.

[4] D. Kune, J. Backes, S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," in *Security and Privacy (SP), 2013 IEEE Symposium on*, 2013, pp. 145–159.

[5] I. Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim, A. King, M. Mullen-Fortino, S. Park, A. Roederer, and K. Venkatasubramanian, "Challenges and research directions in medical cyber physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 75 –90, jan. 2012.

[6] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *Trans. Info. Tech. Biomed.*, vol. 14, no. 1, pp. 60–68, jan 2010.

[7] U. Author, "Mint," http://investorjunkie.com/54/mint-com-review/, 2014.

[8] K. K. Venkatasubramanian, "Security solutions for cyber physical systems," 2009, PhD Thesis, Arizona State University.

[9] S. A. Crosby and D. S. Wallach, "Efficient Data Structures For Tamper-Evident Logging." *USENIX Security Symposium*, Jan. 2009.

[10] R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance." *FAST*, 2009.

[11] P. Maniatis and M. Baker, "Secure History Preservation Through Timeline Entanglement," Feb. 2002.

[12] R. J. Walls, B. N. Levine, M. Liberatore, and C. Shields, "Effective Digital Forensics Research is Investigator-Centric," in *Proc. USENIX Workshop on Hot Topics in Security (HotSec)*, August 2011. [Online]. Available: http://forensics.umass.edu/pubs/Walls.hotsec.2011.pdf

[13] S. Nabar, A. Banerjee, S. K. S. Gupta, and R. Poovendran, "GeM-REM: Generative model-driven resource efficient ecg monitoring in body sensor networks," in *Body Sensor Networks (BSN), 2011 International Conference on*. IEEE, 2011, pp. 1–6.

[14] ——, "Resource-efficient and reliable long term wireless monitoring of the photoplethysmographic signal," in *Proceedings of the 2nd Conference on Wireless Health*, ser. WH '11. New York, NY, USA: ACM, 2011, pp. 9:1–9:10.

[15] A. Banerjee, S. K. S. Gupta, and K. K. Venkatasubramanian, "Pees: Physiology-based end-to-end security for mhealth," in *Proceedings of the 4th Conference on Wireless Health*, ser. WH '13. New York, NY, USA: ACM, 2013, pp. 2:1–2:8. [Online]. Available: http://doi.acm.org/10.1145/2534088.2534109

[16] P. Asare, D. Cong, S. G. Vattam, B. Kim, A. King, O. Sokolsky, I. Lee, S. Lin, and M. Mullen-Fortino, "The medical device dongle: An open-source standards-based platform for interoperable medical device connectivity," in *Proceedings of the 2Nd ACM SIGHIT International Health Informatics Symposium*, ser. IHI '12, 2012, pp. 667–672.

[17] J. Sorber, M. Shin, R. Peterson, C. Cornelius, S. Mare, A. Prasad, Z. Marois, E. Smithayer, and D. Kotz, "An amulet for trustworthy wearable mhealth," in *Proceedings of the Twelfth Workshop on Mobile Computing Systems &#38; Applications*, ser. HotMobile '12, 2012, pp. 7:1–7:6.

[18] S. Marceglia, P. Fontelo, and M. J. Ackerman, "Late breaking research abstract: A standards-based architecture proposal for integrating patient mhealth apps to electronic health record systems," in *Proceedings of the Wireless Health Conference 2014*, ser. Wireless Health '14, 2014.

[19] "Physiobank," http://www.physionet.org/physiobank/.

[20] M. Unser and A. Aldroubi, "A review of wavelets in biomedical applications," *Proc. of the IEEE*, vol. 84, no. 4, pp. 626–638, 1996.

[21] J.-A. Jiang, C.-F. Chao, M.-J. Chiu, R.-G. Lee, C.-L. Tseng, and R. Lin, "An automatic analysis method for detecting and eliminating ECG artifacts in EEG," *Computers in biology and medicine*, vol. 37, no. 11, pp. 1660–1671, 2007.