nymi™

WHITE PAPER

08.11.2015

This white paper provides the reader with an overview of the Nymi Band and how it works.

We have included information about its development, functioning, underlying technology, security and privacy.

Contents

Preface 1

Introduction 2

- Redefining Identity 2
- How does the Nymi Band Work? 4
  - Sensors 4
  - Closing the Loop – Enrollment and Activation 5
  - Communication 7

The HeartID Technology 8

- ECG Recognition 8
  - Introduction 8
  - History of ECG as a Biometric 10
- ECG Verification and Pattern Recognition 12
- Heart Conditions and Rate Fluctuations 13
  - Why HeartID is not a Monitoring System 14

Security 15

- Threat Model and Guaranteed Security Properties 15
  - Impersonation 15
  - Passive Eavesdropping 16
  - Malleability of Communication 16
  - Tracking and Privacy 16
- Multi-Factor Authentication 17
  - Biometric Authentication 17
  - Possession of the Nymi Band 17
  - Possession of the Nymi Companion Application 17
- Cryptographic Protocols 19
  - Secure Pairing and Communication 19

Owner Identity Confirmation and Digital Signing 20
Random Key Generation and Storage 21
Tracking Prevention and Broadcasting 22
Hardware Security 22
Privacy 23
Privacy by Design 23
Proactive 24
Default 24
Embedded 24
Full Functionality 24
End-to-End Security 25
Transparency 25
Respect 25
Data Storage 26
Opt-in Process 26
Privacy vs. Proximity 26
Conclusions 28
References 29
Glossary 32

Preface

The Nymi Band™ is a wearable device that is the central component of a unique platform to enable Secure, Continuous Authentication. It addresses the security and convenience problems of today, while enabling a hyper-personalized user experience for the emerging applications of tomorrow. The mechanism to deliver this capability is HeartID™, Nymi's proprietary technology that authenticates the wearer using their electrocardiogram (or ECG).

The following white paper aims to explain what the Nymi Band is, how it works, its development, and its underlying technologies. It also provides an overview of possible security attacks and the measures the Nymi Band employs to deter them. Finally, the paper provides a description of our privacy model and how a Nymi Band user controls their data storage and access.

It is important to note that this document is not intended to provide detailed technical specifications or information about how the Nymi Band's software components interface. Application developers should refer to our API and additional developer documentation available at www.nymi.com/dev.

Introduction

Redefining Identity

From government-issued identity documents and payment cards, to passwords and PINs, our daily lives are scattered with tools for modern existence. Each additional tool introduces a supplementary point of friction throughout our day. This cumulative friction is reaching significant proportions, as we continue to accumulate even more keys and cards in our wallets and struggle to remember increasing numbers of passwords for our accounts. Moreover, all of these items, physical or logical, may be stolen or compromised. Aside from the inconvenience and risk they inflict, one characteristic ties these tools together: they all represent different mechanisms for communicating our identity. In essence, their central purpose is to confirm that we are who we claim to be. Practically speaking, we don't own our own identity tools – they are imposed upon us – even though we are constantly engaged in organizing and maintaining them. A solution to simplify our lives and redefine what identity means is desperately needed.

With the Nymi Band, Nymi is introducing a new concept: continuous authentication on the body. The Nymi Band is a lightweight wristband that acts as the central point of identity for its user. It incorporates various security features, including the use of cardiac rhythm as a factor of seamless biometric authentication. Acting as an extension of the user, the Nymi Band becomes a trusted provider of their identity. As soon as it is removed from the wearer's body, it becomes deactivated. This feature allows a user's identity to persist until the removal of the device from the body, a concept Nymi refers to as "Secure, Continuous Authentication".

What makes the Nymi Band unique as a system and platform is that it separates the action of identity authentication from the transactions that rely on it, making it possible for the individual to only need to confirm their identity once a day. The wearer is authenticated

when they first put on the wristband, which enables continuous and reliable access to devices and services, via secure Bluetooth communication and in the future, via other forms of communication. Trusted identity recognition, combined with proximity detection and gesture control, provides the Nymi Band wearer with seamless, privacy-protected, and secure interactions.

While it's easy to view the Nymi Band exclusively as a security or convenience tool as a provider of persistent identity on the body, it opens a much broader range of possibilities. Ultimately, the Nymi Band is a platform that puts identity at the centre of our daily interactions, enabling hyper-personalized user experiences. With the growing integration of smart technologies in our travel, domestic and service environments, the possibilities for future applications are endless. This level of personalization makes the Nymi Band ideal for service industries (i.e. hospitality and tourism), retail stores, corporate and government offices, in addition to homes and personal accounts. The Nymi Band will be the key to the future of smart technology and seamless user experiences.

How does the Nymi Band Work?

SENSORS

The Nymi Band is a wristband with an electronics module, called the Nymi Core, which incorporates an ECG sensor with two electrodes – located on the top and bottom of the module. One electrode touches the wrist, and one is exposed on the top side of the Nymi Core. ECG data can be captured when the user wears the Nymi Band on one wrist and touches the top electrode with the opposite hand.

The Nymi Band also incorporates a six-axis motion sensor (accelerometer and gyroscope), which is used for simple user tap input. In the future, these sensors can be used for applications such as activity tracking (e.g. pedometer, sports, fitness, etc.) and gesture recognition (e.g. unlocking a door or turning on a light). The motion sensor includes a motion co-processor, which may support a variety of motion analytics via future firmware upgrades.

CLOSING THE LOOP – ENROLLMENT AND ACTIVATION

The Nymi Band achieves its functionality through the Nymi Companion Application (NCA), which runs on the user's smartphone, tablet, or computer. The NCA serves as an interface which allows the user to both enroll and authenticate with the Nymi Band.

Enrollment is the process of capturing and processing a sample of the user's ECG in order to turn it into a biometric template. The enrollment process is initiated and performed from the NCA; the user's ECG is captured from the Nymi and transmitted wirelessly to their NCA over a secure channel. Their biometric template is stored on the NCA in an encrypted form so that it cannot be compromised even if the NCA is compromised.

Activation is the process of authenticating the user's identity against the previously created biometric template. As with enrollment, activation is performed by capturing the user's ECG from their Nymi Band and transmitting it to their NCA. The live ECG sample is matched in real-time against the biometric template. If a confident match is achieved within the maximum allowed wait period, then the user is authenticated and the Nymi Band becomes activated. Once in an activated state, the Nymi Band can communicate the user's identity credentials to other devices and systems, termed Nymi Enabled Applications (NEAs). After this initial activation process is completed, the NCA is no longer required, so long as the wristband remains on the user's wrist. Some examples of NEAs are payment

systems, smartphones, tablets, computers, Bluetooth locks, smart appliances, and any Bluetooth enabled device. It should be noted that the Nymi Band does not communicate biometric data to NEAs – it only communicates a digital credential which represents the user's identity.

Future updates to the Nymi Band's firmware will include the ability to authenticate on the band itself, making the use of the NCA optional for routine authentication.

COMMUNICATION

The Nymi Band incorporates a Bluetooth 4.0 Low Energy (BLE) radio for wireless communication. BLE is employed for all communications between the Nymi Band, NCAs and NEAs. In addition to transmitting information, BLE is leveraged to perform proximity detection.

The HeartID Technology

ECG Recognition

INTRODUCTION

A biometric is defined as a behavioural or physiological characteristic that is used to recognize a person's identity. In order for a biometric to be effective, it must be universal, unique for each individual in the population, and stable over time[1]. One of the earliest biometrics used were fingerprints because they were mostly universal, unique, permanent, and easy to capture. More recently, facial recognition has become common for applications ranging from access control to surveillance. One of the challenges associated with these biometrics is that they can often be lifted or captured without a person's consent (known as skimming).

Electrocardiograms (ECGs), by comparison, cannot easily be captured without cooperation from the person. ECG is the electrical signal generated by the heart. It requires direct or very close contact with the user, making it perfect for user-controlled biometric recognition systems. Unlike fingerprints, latent samples are not left behind on contact surfaces. Additionally, ECG can be captured in a way that is still very seamless and convenient for the user.

Standing research supports the use of ECG as a biometric to reliably distinguish people[2-8, 13-15]. The distinctive patterns present in an ECG signal are a result of several factors of the cardiac function that control how the wave is depicted. Electrophysiological variations of the heart muscle, such as its size and position, along with the timing of blood pumping in

and out of the heart, add to the unique properties of every person's ECG waveforms[5].

Among the strengths of ECG in biometric recognition is its continuous property. Unlike iris or fingerprint images that can be scanned at a single point in time, the ECG signal has a constant flow that allows it to be continuously reassessed to identity a user. The inconvenience with traditional biometric systems, such as the fingerprint technologies, is that when the system rejects a user, the user has to swipe or scan their fingers again for their claim to be reconsidered. Using ECG eliminates this inconvenience by collecting the signal continuously until the device is confident it has a match, which also allows the system to opt for high accuracy and continuous authentication.

Leveraging these inherent benefits of the ECG signal, the HeartID technology employs cutting edge signal processing and machine learning algorithms to uniquely identify a person using their ECG biometric.

HISTORY OF ECG AS A BIOMETRIC

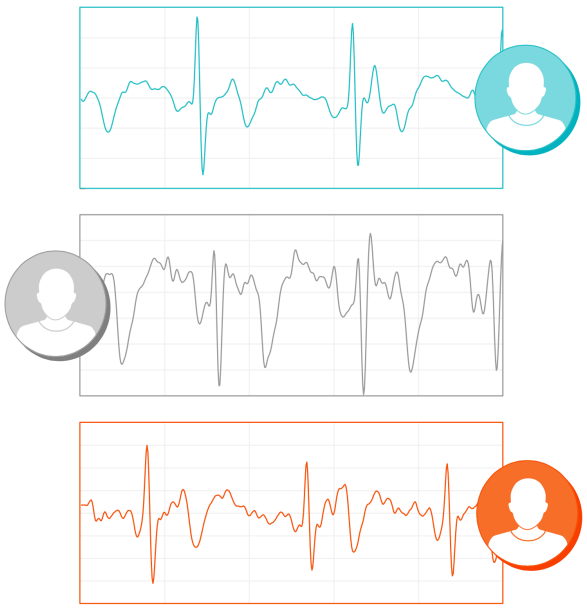
ECG has come a long way since its development by Nobel Prize winning physiologist Willem Einthoven in the early 20th century[16]. Since that time, it has become an indispensable tool in clinical cardiology and is one of the most widely used signals in healthcare. Recorded at the surface of the body, with electrodes attached in various configurations, the ECG signal is studied for diagnostics. In essence, this signal describes the electrical activity of the heart over time. The output is in the form of a wave that depicts an individual's unique internal heart rhythm.

The ECG signal is a relatively new addition to the biometric family. Interestingly, because different individual's ECGs vary with such significance, the medical community has had difficulty creating diagnostic standards for medical applications. Although the unique properties and characteristics of ECG signals had been observed before and ideas of biometric applications were discussed in 2001, the process of gathering data was complicated. Some of the earliest research in the field demonstrated the feasibility of using ECG signals from subjects of various ages and experimenting with electrode placement[11,12]. These early reports on ECG biometrics focused on the extraction of distinctive characteristics from ECG waves, without much consideration for how the technology could be practically applied.

Similar to facial recognition, early efforts in ECG technology were focused on creating points of reference for authentication (also known as the fiducial approach[13]). Like measuring the distance between a person's eyes or the length of their nose, ECG waves were analyzed in terms of the relative distances between points and the duration of inter-beat intervals. From 2007, systematic efforts from Professor Dimitrios Hatzinakos' group at the University of Toronto led the way to analyzing the overall ECG waveform instead of distinct points of reference for ECG recognition (also known as the non-fiducial approach[9]). Recently, both fiducial and non-fiducial approaches have been utilized for ECG biometric[14].

HeartID's ECG biometric originated from the extensive research conducted at the University of Toronto[9]. The original algorithm has been shown to outperform most contemporary ECG biometric systems[12,15]. Since its creation, the system has evolved significantly by deploying the latest advances in the fields of signal processing and machine learning. It has now matured to deliver the most robust and efficient commercially available ECG biometric authentication system.

ECG Verification and Pattern Recognition



While healthy ECG signals from different people conform to roughly the same repetitive pulse pattern, small differences in the overall shape of their waves reveal significant distinctions between individuals (as illustrated in the figure to the right). During the authentication process, HeartID is able to discard noise from recording artifacts that result from breathing, body movement or an inadequate connection and instead focuses on pattern recognition to either accept or reject the user. HeartID's pattern recognition engine uses a unique hybrid of fiducial and non-fiducial type features extracted from ECG. This allows the ECG wave to be analyzed for repeated unique patterns while factoring out artifacts and incidental forms. Following this, machine learning techniques are employed to improve detection of the user's unique ECG signature. During enrollment, HeartID extracts features which are persistent in an individual's ECG and at the same time distinguishable amongst a population.

Heart Conditions and Rate Fluctuations

Medical heart conditions such as cardiac arrhythmias, arterial fibrillations, or implants (e.g., pacemakers) do not impact HeartID's performance. Every heartbeat, even an irregular one, has a unique signature[4]. Because these conditions are persistent, HeartID's pattern recognition engine learns the condition and includes it as part of the user's biometric template[4].

In addition, mild variations in heart rate caused by activities such as moderate exercise, consuming caffeine or taking medication do not impact HeartID's ability to authenticate the user. During the authentication process, the system is able to ignore low frequency anomalies and can still correctly identify the enrolled user.

If an individual experiences a severe cardiac event that significantly alters their ECG, they can update their biometric template using a secure process. HeartID can use this updated template to recognize the individual.

WHY HEARTID IS NOT A MONITORING SYSTEM

The existing HeartID system is not a continuous heart monitoring or medical device, and cannot be used to diagnose medical conditions. The signal retrieved and processed by the HeartID system is customized for biometric purposes only. It is possible that future generations of HeartID could expand to include medical capabilities.

Security

Ensuring the Nymi Band is secure and protected from violations is a primary focus for the existing product, and future updates. As biometric recognition becomes increasingly popular, the fear of circumvention, obfuscation and replay attacks is a rising concern. Unlike fingerprints or iris scans, which can be easily forged or replicated, ECG is a vital signal of the body, and as such, it naturally provides strong protection against intrusions and falsification. Furthermore, substantial security measures for both the hardware and software components, to defend against tracking, spoofing and hacking, will be integral to the Nymi Band ecosystem. Individuals are providing access to their lives through their Nymi Band, and Nymi has created a protected trust chain that aims to make it impossible for others to exploit or compromise that trust.

Threat Model and Guaranteed Security Properties

When designing a security system, it is important to keep in mind that adversaries do not adhere to a set of rules. An attacker may be willing to utilize any means necessary and use unconventional methods to gain unauthorized access to the system16. The types of attacks prevented by the Nymi Band are described below. Details on how these security properties are achieved are provided in the section “Cryptographic Protocols”.

IMPERSONATION

An impersonating adversary could attempt to mimic the functionality of their target’s Nymi Band; for example, by trying to activate it. The Nymi Band is a multi-factor system, and as a result it will remain resilient to impersonation as long as at least one factor has not been compromised. Furthermore, impersonation of another person’s ECG is exceedingly difficult to execute.

PASSIVE EAVESDROPPING

An eavesdropper is an adversary that passively listens to radio communication links and attempts to discern valuable information from the raw data that is being transmitted. The Nymi Band is designed to be completely impervious to passive eavesdroppers.

MALLEABILITY OF COMMUNICATION

A powerful type of adversary may be able to modify radio communications between the Nymi Band and its communication partner devices (NCA or NEA). This can be achieved by employing sophisticated and costly hardware strategies such as high-powered transmitters. Such an adversary can completely congest communication, or attempt to surreptitiously modify it in order to make the link insecure, thereby enabling one of the attacks described above. The Nymi Band also provides protections for high value transactions against relay attacks, where the adversary uses transmitters to covertly extend the communication range of the victim's Nymi Band. While entirely preventing active attacks is not possible, the Nymi Band is resilient to a wide range of active assaults, including the most plausible 'man-in-the-middle' strategy.

TRACKING AND PRIVACY

In the modern age of information, the privacy of individuals is of the utmost importance. The Nymi Band was designed with privacy as a foundational pillar, and is therefore one of the most secure smart mobile devices available. A tracking adversary can observe radio communications in multiple geographic locations, and may even attempt to send transmissions to devices, in an effort to trigger a response that will reveal their identity. The Nymi Band ensures user privacy by employing robust cryptographic techniques. These techniques guarantee that only the devices the Nymi Band has been paired with can detect its presence. The owner of the Nymi Band can freely go about their daily life, including travel, without leaving any identifiable trace of their route.

Multi-Factor Authentication

The Nymi Band is inherently a multi–factor authentication system; each factor the Nymi Band employs adds a deeper layer of protection against impostors.

BIOMETRIC AUTHENTICATION

ECGs are extremely difficult to capture and replicate. To bypass biometric authentication, the impostor would need to simulate the owner's ECG.

POSSESSION OF THE NYMI BAND

The Nymi Band would have to be stolen in-tact, as breaking the band is detected via a sensing mechanism that informs the system the wristband has been cut, and prevents the device from working. Unclasping or cutting of the wristband invalidates biometric authentication.

POSSESSION OF THE NYMI COMPANION APPLICATION

The device with the NCA installed needs to be present while activation is being performed. In addition to spoofing the Nymi Band, the potential con artist would also

have to steal and access the user's device with the NCA in order to attempt to activate the stolen Nymi Band. Note that this device does not need to be present after successful activation of the Nymi Band.

An adversary that wishes to fraudulently put another person's Nymi Band into the activated mode must gain possession of the undamaged Nymi Band and the device with the NCA, and then also spoof the owner's cardiac signature. There is currently no known means of falsifying an ECG waveform and presenting it to a biometric recognition system.

Cryptographic Protocols

When a user activates their Nymi Band using their ECG, it becomes a trusted device that acts as an extension of the individual to securely communicate their identity. One of the distinguishing characteristics of the Nymi Band is its strong underlying cryptographic foundations. All of the security guarantees provided by Nymi are backed by well-established and time-tested cryptographic primitives[17–20]. While encryption can theoretically be broken, the Nymi Band is designed to rely on the same algorithms that protect e-commerce transactions on the Internet, banking information, and classified government material. An attack on the Nymi Band's communication and authentication protocols would imply an attack on all of these high value systems. Moreover, the Nymi Band's cryptography is regularly updated to be aligned with the latest research and standards. The Nymi Band employs the following cryptographic tools and counter-measures:

SECURE PAIRING AND COMMUNICATION

When the Nymi Band is introduced to a new Nymi Enabled Application (NEA), a secure pairing protocol is performed. Pairing is achieved by executing a Hashed Diffie-Hellman key exchange, and then using the resulting session key to transmit a long-term key from the Nymi Band to the NEA. All communication is encrypted and authenticated using the long-term key from that point forward.

The Nymi Band's pairing protocol guarantees long-term security against eavesdropping adversaries, both during the pairing phase and any future interaction with the NEA. The protocol also guarantees that any active 'man-in-the-middle' (MIM) adversary must continue to actively modify radio communication between the Nymi Band and the third party device at all times to avoid detection and termination of the pairing. Active MIM attacks in a radio communications setting are extremely difficult and costly to perform.

OWNER IDENTITY CONFIRMATION AND DIGITAL SIGNING

A feature of the Nymi Band is the ability for its owner to publicly identify him or herself and securely digitally sign transactions. The Nymi Band has the capability of using a built-in hardware based elliptic curve Digital Signature Algorithm (ECDSA), to securely generate pairs of public and private keys[21,22]. Using these private keys, signatures of transactions can be computed.

The most common factor of authentication after passwords is “secure tokens”, which require a key that must be stored in both the device and on a remote authentication server. These servers become attractive targets for adversaries. The Nymi Band circumvents this issue by using public key cryptography, meaning there is only one copy of the secret key, which is stored in the Nymi Core. As a result, in order to hack a system that relies on the Nymi Band for authentication, the attacker must physically steal the Nymi Band, which would likely be discovered by its owner. In contrast, when a “secure token” with a stored key on remote server is attacked, the victim has no way of knowing that their secret key was stolen.

One of the most challenging aspects of utilizing public key cryptography is the necessity of keeping the private keys private. In essence, this guarantees that under no circumstances will an adversary be able to gain access to someone else’s private key. The digital signing mechanism of the Nymi Band is designed so that the private keys never physically leave the Nymi Band, thereby guaranteeing that no one can fake the owner’s signature. In addition, the keys are stored in a secure hardware element on the Nymi Band, making it extremely costly and difficult for attackers who managed to gain physical possession of the device (for example, by stealing it) to access the keys. Furthermore, the Nymi Band will never store any code locally other than its own trusted firmware, eliminating the risk of rogue programs exfiltrating secret keys. The implementation of the Nymi Band’s digital signing capabilities approaches the ideal mathematical models that provide strong provable security and have withstood the test of time, as closely as possible.

RANDOM KEY GENERATION AND STORAGE

Block-ciphers such as AES are widely used in practical applications[23, 24]. The Nymi Band provides a secure and convenient facility to manage cryptographic keys used by such applications. To enable the correct use and storage of block-cipher keys, the Nymi Band provides a hardware-based facility that allows applications to use it to generate random keys, and then retrieve them when necessary. This allows the Nymi Band to function as a secure encryption key ring for its owner that can be carried at all times. Unlike other methods of storing keys, such as USB drives, the Nymi Band does not act as a drive. Instead, it only exposes the appropriate cryptographic API, preventing scenarios where the key storage is infected by malicious software present on a connecting NEA.

TRACKING PREVENTION AND BROADCASTING

As a connected and transmitting device that is constantly worn by its owner, the Nymi Band was designed for privacy and to prevent any type of tracking or unwanted identification. As the user goes about their daily activities, the Nymi Band broadcasts what appears to be random noise that lacks any pattern or structure. Only NEAs that the Nymi Band has been paired with can detect its presence and engage in communication. This is achieved by having the Nymi Band broadcast an encrypted randomized message under each of the long-term keys that were established during the pairing process. The devices that the Nymi band was paired with attempt to decrypt incoming random communication, and only if decryption is successful will they send back an authenticated message requesting to begin communicating. In turn, the Nymi Band ignores all attempts for open communication that are not properly authenticated by one of its paired devices (NEAs) - unless the Nymi Band is in pairing mode.

Hardware Security

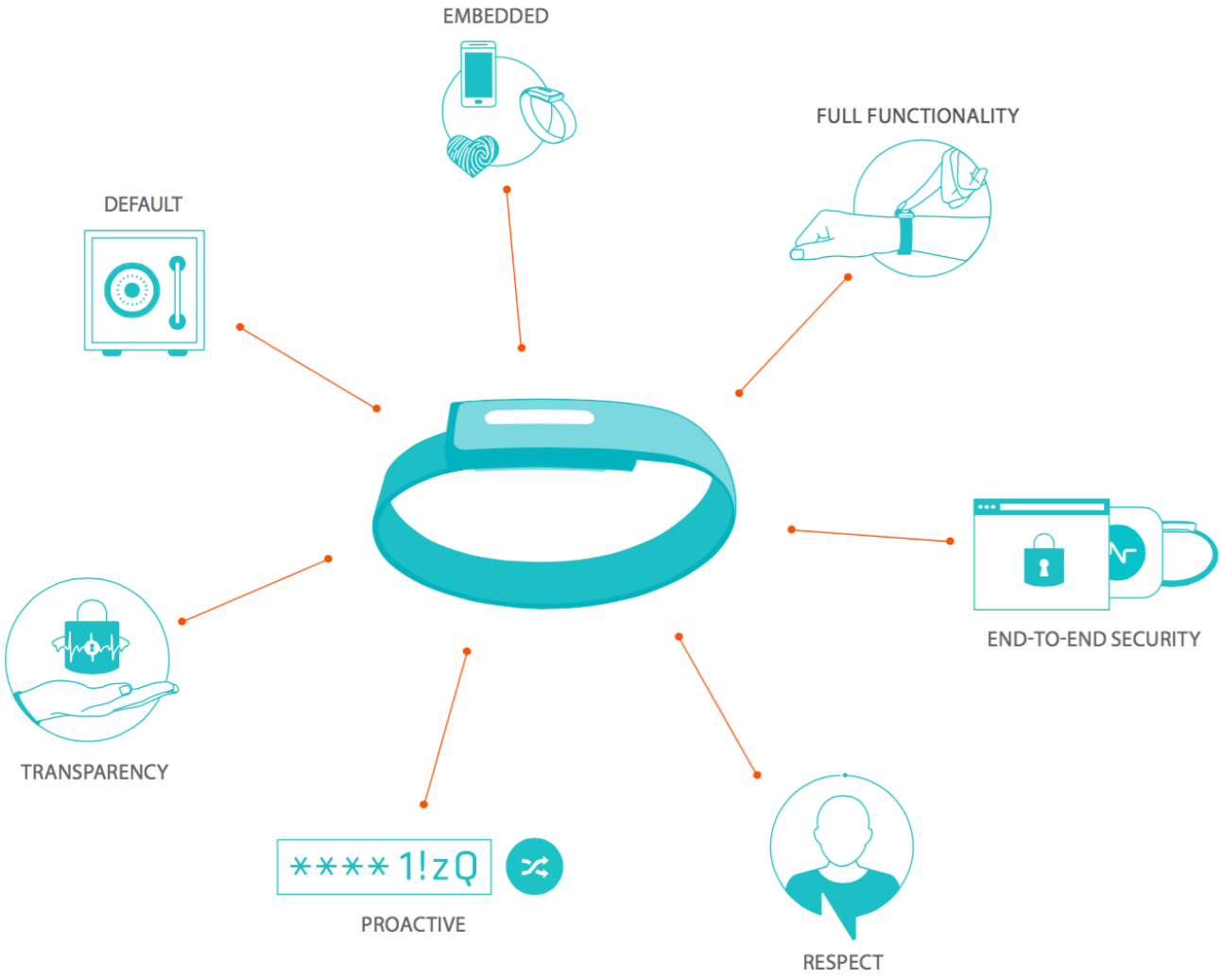
The Nymi Band has multiple hardware security features that protect its user's data in case the device is lost or stolen. To detect removal of the Nymi Band from its wearer's wrist, the Nymi Band has the ability to effectively sense separation from the wearer. If the Nymi Band is removed from the wrist or cut, the system will immediately detect the intrusion and the Nymi Band will go into the inactivated, preventing access to any internal data.

The Nymi Band also contains a secure hardware element with countermeasures against physical tampering. All of the keys that protect the owner's data and are used for activation are kept in secure storage on the hardware element. This provides protection against attackers who have gained physical possession of the device and are attempting to access the information inside the stolen Nymi Band.

Privacy

Privacy by Design

During the Nymi Band's design process, Nymi adopted the set of Privacy by Design standards developed by the Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian. Privacy by Design is the intentional planning of a product in such a way that privacy controls become integral to the design of the technology[25]. The Nymi Band has been engineered to ensure that it's both secure and privacy-protected from end-to-end, without requiring any action on behalf of its owner.



PROACTIVE

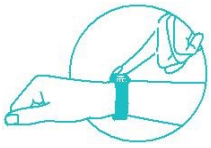
The Nymi Band is designed with the end-users privacy as the top priority, to prevent privacy breaches before they arise through secure pairing, random key generation, digital signing, and tracking prevention.

DEFAULT

The user's ECG and access to their accounts and devices are automatically protected through the complex encryption and security measures outlined in the Security section. The Nymi Band is designed so that the user does not have to take any action to protect their privacy; encryptions and protective protocols are automatic.

EMBEDDED

Through local data storage, hardware security and Multi-Factor Authentication, the Nymi Band is designed with protective privacy features embedded directly into the product. Privacy protection attributes, such as the secure hardware element, are an integral part of the underlying structure of the Nymi Band.



FULL FUNCTIONALITY

Both security and privacy are essential to the functionality of the Nymi Band. Secure communications between the Nymi band, the user, and NEAs are critical to ensuring the

owner's privacy. The cryptographic protocols the Nymi Band employs provide equal weight for both security and privacy.

END-TO-END SECURITY

Data is securely collected and transmitted from enrollment to activation to communication, through secure pairing, random key generation, digital signing, and tracking prevention. Local storage of keys make attacks on remote authentication servers impossible and device reporting adds a deeper layer of protection.

TRANSPARENCY

Nymi operates the Nymi Band according to our guaranteed security properties. The opt-in data process ensures users maintain control of their information and access at all times. A user cannot be tracked or identified by third-party devices, without the owner explicitly pairing them with their Nymi Band.

RESPECT

Through our privacy and security protocols, the Nymi Band is designed with the intention of creating a device which empowers the owner to control their own identity and security. Override functions and security architecture provide the user with a personalized experience that is privacy-protected.

Data Storage

The Nymi Band does not retain any tracking or personal information about its owner. In addition, the cryptographic keys that are used by the Nymi Band are stored in a tamper-resistant, secure hardware element. In the event a user's Nymi Band is lost or stolen, an attacker would have to invest considerable resources and time to extract any information from the Nymi Band. The Nymi Band security architecture is designed so that long term damage can be avoided by reporting a lost Nymi Band through the NCA and revoking all the embedded keys. The NCA maintains a processed version of the owner's ECG template. While the processed template provides no provable guarantees, it is encrypted with the owner's password and a key stored on the Nymi Band. In addition, it is protected by the security mechanisms of the NCA; for example, iOS or Android security.

Opt-in Process

Tracking by third parties is a significant privacy concern for users of all mobile devices with transmitting functions. The Nymi Band is designed to be ubiquitous and wearable at all times, while preserving the anonymity and privacy of its owner. In particular, the design of the communication protocols, employed by the Nymi Band, guarantees that it cannot be tracked or identified by third-party devices, without the owner explicitly pairing them with the Nymi Band. For more details on how tracking prevention and privacy are achieved by the Nymi Band, please refer to the "Cryptographic Protocols" section.

Privacy vs. Proximity

The Nymi Band implements a propriety set of algorithms for proximity estimation based on the Bluetooth signal. The transmitting device (in this case the Nymi Band) transmits a beacon signal along with the transmitting signal strength. The receiving device uses this information, in addition to the received signal strength, to estimate the proximity of the Nymi Band. While the proximity information reveals the presence of an electronic device,

the Nymi Band broadcasts an encrypted signal that is decipherable only by its paired devices[20]. Any attempts to track the owner of the Nymi Band will fail because a third party device that was not paired with the Nymi Band will be receiving a signal that only contains random noise.

Conclusions

The Nymi Band was developed to improve the wearer's daily experience, enabling secure and continuous authentication. Its underlying technology, security and privacy have been designed specifically to provide the end-user with an empowering, easy to use solution to manage their identity. Adaptive to the user's environment and dynamic, the Nymi Band allows its owner to control how they want to integrate the technology into their lives. It is a system that simplifies the user's life by removing complications associated with identity and security.

Protected from monitoring and third-party tracking, the Nymi Band will provide individuals, organizations and groups with secure and seamless interactions for a variety of applications and devices. We expect that users and developers will see the Nymi Band as an opportunity to create hyper-personalized solutions to their needs.

Nymi is committed to working with its developer community to build the future of the Nymi ecosystem. Nymi's developer portal is a platform for developers to voice their interests and work together to bring their application concepts to reality.

As a team of eager engineers, scientists and thought-leaders, Nymi aims to shape the world using novel concepts and technologies. Its brainchild, the Nymi Band, redefines identity for the modern world.

References

1. Jain, A. K., Bolle, R., Pankanti, S. “Biometrics: personal identification in networked society”. Kluwer Academic Publications. 1999.

2. Wang, Y., Agrafioti, F., Hatzinakos, D., Plataniotis, K. N. “Analysis of human electrocardiogram for biometric recognition”. In EURASIP Journal on Advances in Signal Processing. 2008.

3. Agrafioti, F., Hatzinakos, D. “Fusion of ECG sources for human identification”. In International Symposium on Communications, Control and Signal Processing: ISCCSP. 2008.

4. Agrafioti, F., Hatzinakos, D. “ECG biometric analysis in cardiac irregularity conditions”. In Signal, Image and Video Processing. 2009.

5. Agrafioti, F., ECG in Biometric Recognition: Time Dependency and Application Challenges, Doctoral Thesis, University of Toronto, 2011

6. Sam Raj, P., ECG Biometrics using Intuitive Bases and Support Vector Machines, University of Toronto, 2014.

7. Pouryayevali, S., Wahabi, S. ; Hari, S. ; Hatzinakos, D. On establishing evaluation standards for ECG biometrics, in IEEE conference on Acoustics, Speech and Signal Processing, 2014.

8. Ikenna Odinaka, Po-Hsiang Lai, AlanD.Kaplan, Joseph A. O’Sullivan, Erik J. Sirevaag, and John W. Rohrbaugh. ECG. Biometric Recognition: A Comparative Analysis, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 6, December 2012.

9. Van Oosterom, A., Hoekema, R., Uijen, G. J. “Geometrical factors affecting the

interindividual variability of the ECG and the VCG". In Journal of Electrocardiolgy. 2000.

10. Sornmo, L., Laguna, P. "Bioelectrical signal processing in cardiac and neurological applications". Elsevier Academic Press. 2005.

11. Biel, L., Pettersson, O., Philipson, L., Wide, P. "ECG analysis: a new approach in human identification". In IEEE Transactions on Instrumentation and Measurement. 2001.

12. Wübbeler, G., Stavridis, D., Kreiseler, R., Bousseljot, R., Elster, C. "Verification of humans using the electrocardiogram". In Pattern Recognition Letters. 2007.

13. Israel, S. A., Irvine, J. M., Cheng, A., Wiederhold, M. D., Wiederhold, B. K. "ECG to identify individuals". In Journal of Pattern Recognition. 2005.

14. Pereira Coutinho, D., Silva, H. ; Gamboa, H. ; Fred, A. ; Figueiredo, M., Novel fiducial and non-fiducial approaches to electrocardiogram-based biometric systems, in Biometrics, IET , 2013.

15. Carlos Carreiras, Andre Lourenc, Ana Fred, Rui Ferreira, "ECG Signals for Biometric Applications Are we there yet?", in International Conference on Informatics in Control, Automation and Robotics, 2014.

16. Stallings, W. "Network security essentials". Prentice-Hall Inc. 1999.

17. Diffie, W., Hellman, M. "New directions in cryptography". In IEEE Transactions on Information Theory. 1976.

18. Goldreich, O., Goldwasser, S., Micali, S. "How to construct random functions". In Journal of the ACM. 1986.

19. Goldwasser, S., Micali, S. "Probabilistic encryption". In Journal of Computer and System Sciences. 1984.

20. Rabin, M. O. “Digitalized signatures and public-key functions as intractable as factorization”. MIT Technical Report. 1979.

21. Federal Information Processing Standards (FIPS) Publication. 186-3. Digital Signature Standard. 2009.

22. Federal Information Processing Standards (FIPS) Publication. 186-4. Digital Signature Standard. 2013.

23. Federal Information Processing Standards (FIPS) Publication. 197. Advanced Encryption Standard. 2001.

24. Daemen, J., Rijmen, V. “AES proposal: Rijndael”. In First Advanced Encryption Standard (AES) Conference. 1998.

25. Cavoukian, A. “Privacy by design”. http://www.ipc.on.ca/images/Resources/privacybydesign.pdf . 2009.

26. Ryan, M. “Bluetooth: with low energy comes low security”. In USENIX Workshop of Offensive Technologies. 2013.

Glossary

Access

The successful communication of a person's identity to the device or application they want to use. For example, a person accesses their front door using their unique key or a Nymi Band user accesses (unlocks) their computer using their activated Nymi Band.

Activation

The process of authenticating the Nymi Band user's identity by communicating their ECG wave to their device with the NCA installed.

Nymi Companion Application (NCA)

Nymi's own application run on a smartphone, tablet, or computer, which facilitates enrollment and activation of the Nymi Band. The NCA also allows the user to access their NEAs. Versions of the NCA are being developed for Android and iOS devices, as well as Windows and Mac computers.

Biometirc

A universal behavioral or physiological characteristic that is used to identify a person.

Block-cipher

A pseudo-random function which transforms a key and a block of data into a value that cannot be distinguished from a completely random sequence of bytes. The output is the same size as the data, and the original data can be recovered from the output given the key. Block-ciphers can be used, in conjunction with appropriately generated randomness, to construct symmetrical encryption algorithms.

Cryptography

The science of identifying and formally defining security requirements of systems, and satisfying these requirements using algorithms that are based on solid mathematical foundations.

Electrocardiogram (ECG)

An interpretation of changes in the electrical activity of the heart overtime, depicted as a wave. Information for an ECG is collected by placing electrodes externally on both sides of the body.

Encryption

A randomized algorithm that takes as input a public (or shared) key, randomness, and the plaintext message, and outputs a ciphertext. To be secure, the output of the encryption algorithm on any two different plaintext messages must be indistinguishable.

Enrollment

The process of recording, processing and storing a user's ECG template on their NCA when they first set up their Nymi Band.

Facial recognition

A physical biometric that uses computer programs to identify a person from a digital image using measurements of their facial features.

Fingerprint recognition

A physical biometric that uses algorithms to match the patterns of fingerprint ridges to identify a person.

Hashed Diffie-Hellman exchange

A method of establishing a shared cryptographic key between the Nymi Band and a previous unknown pairing device (potential NEA), over insecure communication channels.

Machine learning

A program that is able to adapt how it processes data over time to become more efficient and accurate.

Man in the Middle attack

An active attack in which an adversary creates independent connections with a user's Nymi Band and an NEA, and relays false messages in order to make the Nymi Band and the NEA agree on an insecure key.

Nymi Enabled Application (NEA)

An application, typically third-party, that is authorized by the user to communicate with the Nymi Band.

Pattern recognition

The process of matching patterns in data that are exactly the same. Private key A secret value, typically part of a public and private key pair, which allows the owner to sign messages or decrypt ciphertexts.

Public Key

The public access code that corresponds to a private access code in an asymmetric encryption system.

Relay attack

An active attack in which an adversary interrupts Nymi Band communications and relays an identical message to a user's NCA or NEA in order to access it without requiring their Nymi Band, for example by extending the range of communication.

Replay attack

An attack in which an adversary attempts to forge a user's identity by attempting to repeat authorized commands by replicating legitimate messages that were previously transmitted between a Nymi Band and an NEA or NCA.

Spoofing

Recreating data to impersonate a communication. For Nymi Band users, an attacker would attempt to mimic their ECG in order to access their applications and devices.

Third party applications/devices

Software or hardware that is compatible with the Nymi Band. For example, an NEA, smartlocks, wireless payment receiving devices, or website authentication platforms.

Tracking

An attack in which an adversary can attempt to observe radio communications, in multiple geographic locations, in order to track their victim.