11-19-2013

This white paper provides the reader with an overview of the Nymi and how it works. We have included information about its development, functioning, underlying technology, security and privacy.

bionym

Contents

Preface

The Nymi is a unique platform that makes persistent identity a wearable technology. 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 based in a wristband that authenticates the identity of the wearer using their unique cardiac rhythm (electrocardiogram – ECG).

The following white paper aims to explain what the Nymi is, how it works, its development, and its underlying technologies. It also provides an overview of possible security attacks and the measures the Nymi employs to deter them. Finally, the paper provides a description of our privacy model and how a Nymi 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's software components interface. If you're a developer, please refer to our API and additional developer documentation.

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 ever 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 digital, 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 inflicted 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, Bionym is introducing a new concept: persistent identity on the body. The Nymi is a lightweight wristband that acts as the central point of identity authentication. It incorporates various security features, including the use of cardiac rhythm (electrocardiogram - ECG) as a factor of seamless biometric authentication. Acting as an extension of the user, the Nymi becomes a trusted provider of their identity. As soon as it is removed from the wearer's body, it becomes deactivated.

What makes the Nymi 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 services and devices, via wireless communication. Trusted identity recognition, combined with proximity detection and gesture control, provides the Nymi wearer with seamless, privacy-protected, and secure interactions.

While it's easy to view the Nymi 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 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 ideal for hotels, clubs, airports, retail stores, corporate and government offices, in addition to our homes and personal accounts. The Nymi will be the key to the future of smart technology and seamless user experiences.

How does the Nymi Work?

SENSORS

The Nymi is a wristband with an electronics module that 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 dorsal side. ECG data can be captured when the user touches the top-side electrode with the opposite hand.

The Nymi also incorporates a six-axis motion sensor (accelerometer and gyroscope). The captured motion data is used for simple gesture recognition and user input (e.g. tap detection). The gesture recognition may be utilized to indicate the user's intent, such as unlocking the front door of a vehicle versus unlocking the trunk. More generally, the motion data may be used for a variety of applications, such as activity tracking (e.g. pedometer, sports, fitness, etc.). 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 AUTHENTICATION

The Nymi system employs what is known as an Authorized Authentication Device (AAD). An AAD is a smartphone, tablet, or computer, which has the official Nymi companion app installed. Current compatible AAD's include Android and iOS devices, as well as Mac and Windows computers. The AAD allows the user to both enroll and to authenticate.

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

AAD; the users ECG is captured from the Nymi and transmitted wirelessly to their AAD over a secure channel. Their biometric template is stored on the AAD in an encrypted form so that it cannot be compromised even if the AAD is compromised.

Authentication is the process of assessing the user's identity against the previously created biometric template. As with enrollment, authentication is performed by capturing the user's ECG on their Nymi and transmitting it to their AAD. 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 becomes activated. Once in an authenticated state, the Nymi can communicate the user's identity credentials to other devices and systems, termed Nymi Enabled Devices (NEDs). After this initial authentication process is completed, the AAD is no longer required, as long as the wristband remains on the user's wrist. Some examples of NEDs are payment systems, smartphones, tablets, Bluetooth locks, smart appliances, and any Bluetooth enabled device. It should be noted that the Nymi does not communicate biometric data to NEDs – it only communicates a digital credential which represents the user's identity.

COMMUNICATION

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

Underlying 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 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 be easily 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.

Current research supports the use of ECG as a biometric to reliably distinguish people[2–4]. 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, or the timing of blood pumping in and out of the heart, add to the unique properties of every person's ECG waveforms[5].

The Nymi employs ECG recognition as a factor of authentication for the unique combined characteristic of convenience and security, when employed in a wearable form factor. The Nymi thus allows the user to truly take control of their identity.

It should be noted that the technology employed in most heart-rate monitors does not capture ECG. Heart-rate monitors typically use optical sensors to measure blood flow, not

electrical activity. In some cases, this can even be captured at a distance. It cannot, however, be used for biometric recognition using current technology.

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[6]. 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 individuals 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[7,8]. 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.

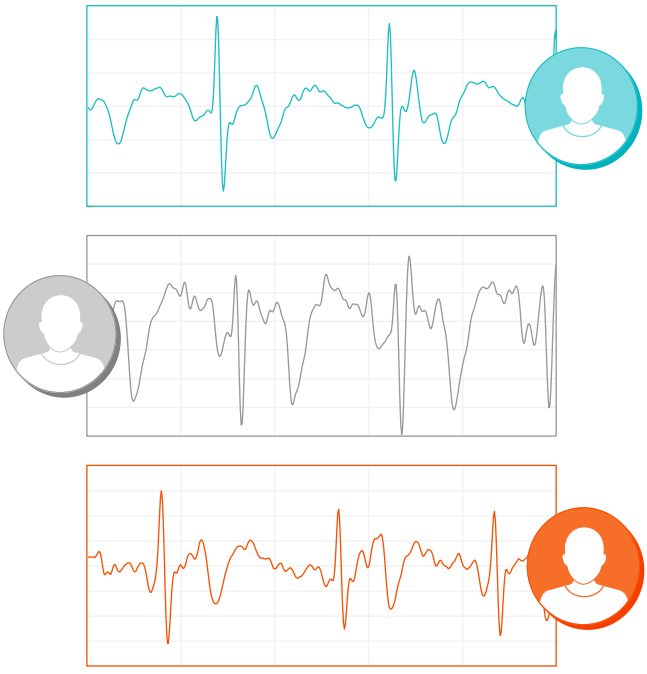
Among the strengths of ECG in biometric recognition is its continuous property. Unlike iris or fingerprint images that can be scanned at a single point in time, the ECG signal has a constant flow that allows the device to reassess the identity of a user continuously. The hassle with traditional biometric 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 annoyance by collecting the signal continuously until the device is confident it has a match.

Similar to facial recognition, early efforts in ECG technology were focused on creating points of reference for authentication. 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[9]. From 2007, systematic efforts from Professor Dimitrios Hatzinakos' group at the University of Toronto, led to the unveiling of a very robust and efficient ECG biometric algorithm that can analyze the overall ECG waveform, instead of creating points of reference[2–4]. This algorithm enabled high-speed analysis, without missing the finest discriminative characteristics of the heartbeats. Out of these advances in research, robust identity authentication using ECG as a biometric was made possible. This is the technology that powers the Nymi.

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. During authentication, the Nymi is able to ignore noise from recording artifacts that result from breathing, body movement or an inadequate connection and instead focus on pattern recognition to either accept or reject the user. Nymi's pattern recognition engine uses a combination of second order statistics to extract unique ECG features. 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 users unique ECG. During enrollment, the Nymi extracts features which are persistent in an individual's ECG and at the same time distinguishable amongst a population.



RELIABILITY OF AUTHENTICATION

The Nymi's ECG biometric system differs from most other biometrics in that it can continuously sample data until a match is found or a timeout occurs. Generally, the accuracy of authentication improves with longer authentications times. The plot in Figure 1 illustrates the accuracy improvement for the Nymi over time. The metric shown is the 'True Accept Rate', which is defined as the percentage of correct verifications of a true identity claim, by the system.

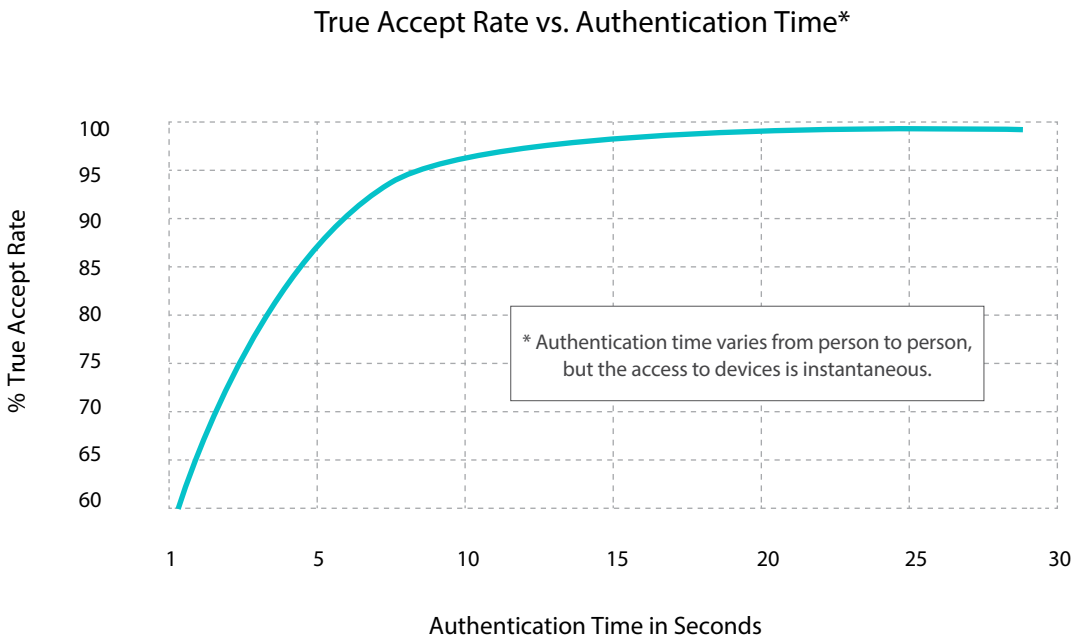


Figure 1. Percentage true accept rate vs. authentication time.

The ECG biometric technology that forms the foundation of the Nymi has been researched and tested extensively over several years[2–4]. With persistent research and development, the reliability of ECG biometrics continues to improve. The use of this biometric technology as one of multiple authentication factors, allows the Nymi to achieve an unmatched level of security without compromising privacy or a convenient user experience.

Heart Conditions and Rate Fluctuations

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

Mild variations in heart rate caused by activities such as moderate exercise, ingesting caffeine or taking medication will not impact the Nymi's ability to authenticate the user. During authentication, the system is able to ignore low frequency anomalies and will still correctly identify its owner. Furthermore, authentication is only performed once when the user puts the wristband on (e.g., at the beginning of the day). During regular usage outside of authentication, the Nymi will be completely unaffected by variations in heart rate. Once the Nymi is authenticated, it becomes an extension of the owner and they can go about their daily activities, including exercising, medicating and accessing all their devices, until they remove the wristband. Once removed, the user will need to go through the authentication process again.

If an individual experiences a severe cardiac event that significantly alters their ECG, they can update their biometric template using a secure process.

WHY THE NYMI IS NOT A HEART MONITORING DEVICE

The first generation Nymi is not a continuous heart monitoring or medical device, and cannot be used to diagnose medical conditions. The wristband does not continuously monitor the user's ECG; ECG is only captured while the user is touching the top electrode with their opposite hand. Furthermore, the Nymi hardware and form factor do not fall into medically approved ECG technology. It is possible that future generations of the Nymi could expand to include medical capabilities.

Security

Ensuring the Nymi is secure and protected from violations is a primary focus for Bionym both during and after product development. 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 ecosystem. Individuals are providing access to their lives through their Nymi, and Bionym 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 system[10]. The types of attacks prevented by the Nymi 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 wristband; for example, by trying to authenticate their victim's Nymi. The Nymi 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 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 and its communication partner devices (AAD or NED). 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 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. While entirely preventing active attacks is not possible, the Nymi 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 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 ensures user privacy by employing robust cryptographic techniques. These techniques guarantee that only the devices the Nymi has been paired with can detect its presence. The owner of the Nymi can freely go about their daily life, including travel, without leaving any identifiable trace of their route.

Three Factor Authentication

The Nymi is inherently a 3-factor authentication system; each factor the Nymi employs adds a deeper layer of protection against impostors.

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

2. POSSESSION OF THE NYMI WRISTBAND
   The Nymi would have to be stolen in-tact, as breaking the band is detected via a sensing mechanism that informs the system the band has been cut, and prevents the device from working. Removal of the wristband invalidates biometric authentication.

3. POSSESSION OF THE AUTHORIZED AUTHENTICATION DEVICE (ANDROID OR IOS)
   The AAD needs to be present while authentication is being performed. In addition to spoofing the wristband, the potential con artist would also have to steal and access the user's AAD in order to attempt to authenticate the stolen Nymi. Note that the AAD does not need to be present after successful authentication.

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

Cryptographic Protocols

When a user authenticates their Nymi using their ECG, the wristband 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 is its strong underlying cryptographic foundations. All of the security guarantees provided by Bionym are backed by well-established and time tested cryptographic primitives[11–14]. While encryption can theoretically be broken, the Nymi 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's communication and authentication protocols would imply an attack on all of these high value systems. Moreover, the Nymi's cryptography is regularly updated to be aligned with the latest research and standards. The Nymi employs the following cryptographic tools and counter-measures:

SECURE PAIRING AND COMMUNICATION

When the Nymi is introduced to a new Nymi Enabled Device (NED), 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 to the NED. All communication is encrypted and authenticated using the long-term key from that point forward.

The Nymi's pairing protocol guarantees long-term security against eavesdropping adversaries, both during the pairing phase and any future interaction with the NED. The protocol also guarantees that any active 'man-in-the-middle' (MIM) adversary must continue to actively modify radio communication between the Nymi 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 is the ability for its owner to publicly identify themselves and securely digitally sign transactions. The Nymi 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[15,16]. 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 circumvents this issue by using public key cryptography, meaning there is only one copy of the secret key, which is stored on the wristband. As a result, in order to hack a system that relies on the Nymi for authentication, the attacker must physically steal the Nymi, 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, guaranteeing 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 is designed so that the private keys never physically leave the Nymi, 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, 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 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'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[17,18]. The Nymi 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 provides a hardware-based facility that allows applications to first generate random keys using the Nymi, and then retrieve them when necessary. This allows the Nymi 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 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 NED.

TRACKING PREVENTION AND BROADCASTING

As a connected and transmitting device that is constantly worn by its owner, the Nymi was designed for privacy and to prevent any type of tracking or unwanted identification. As the user goes about their daily activities, the Nymi broadcasts what appears to be random noise that lacks any patterns or structure. Only NEDs that the Nymi has been paired with can detect its presence and engage in communication. This is achieved by having the Nymi broadcast an encrypted randomized message under each of the long-term keys that were established during the pairing process. The devices that the Nymi 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 ignores all attempts for open communication that are not properly authenticated by one of its paired devices (NED) - unless the Nymi is currently in pairing mode.

Hardware Security

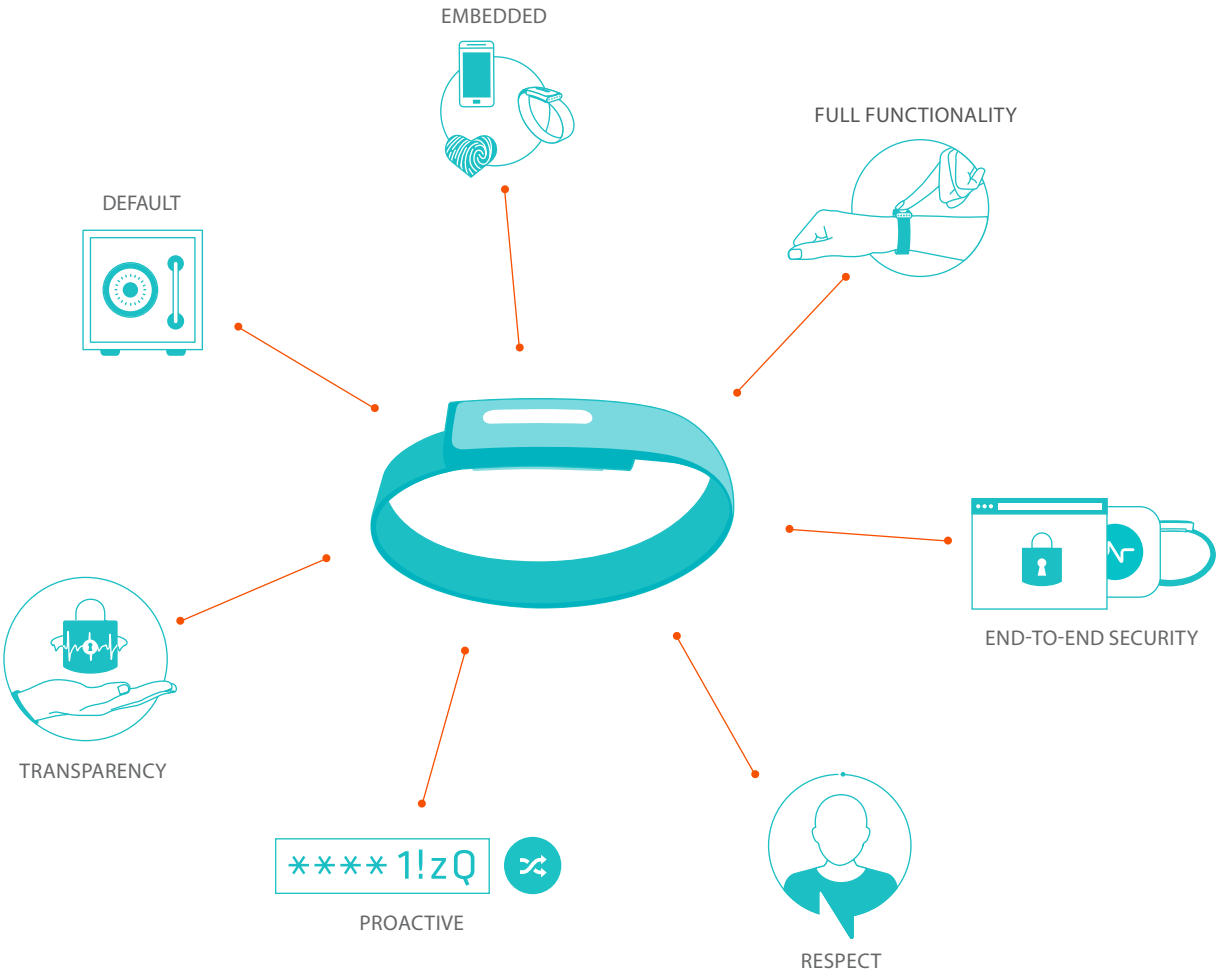
The Nymi has multiple hardware security features that protect its user's data in case the device is lost or stolen. To detect removal of the Nymi from its wearer's wrist, the Nymi has the ability to effectively sense separation from the wearer. If the Nymi is removed from the wrist or cut, the system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

The Nymi 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 authentication 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. While a sufficiently well-funded and equipped adversary may be able to gain access to the keys inside the Nymi after some time, the security architecture of the Nymi allows its owner to report the device as lost or stolen, immediately invalidating the keys in the wristband. By the time the attacker gains access, the keys have become unusable.

Privacy

Privacy by Design

During the Nymi design process, Bionym 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[19]. The Nymi 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

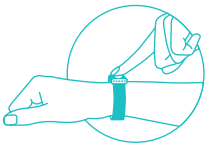
The Nymi is designed with the end-users privacy as the top priority to prevent privacy breaches before they arise through secure pairing, random key generation, digital signing, and tracking prevention.

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 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 Three-Factor Authentication, the Nymi 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.



FULL FUNCTIONALITY

Both security and privacy are essential to the functionality of the Nymi. Secure communications between the Nymi, the user, and NEDs are critical to ensuring the owners privacy. The cryptographic protocols the Nymi employs provide equal weight for both security and privacy.

END-TO-END SECURITY

Data is securely collected and transmitted from enrollment to authentication 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

Bionym operates the Nymi 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.

RESPECT

Through our privacy and security protocols, the Nymi 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 does not retain any tracking or personal information about its owner. In addition, the cryptographic keys that are used by the Nymi are stored in a tamper-resistant hardware element. In the event a user's Nymi is lost or stolen, an attacker would have to invest considerable resources and time to extract any information from the Nymi. The Nymi security architecture is designed so that long term damage can be avoided, by reporting the Nymi lost through the companion app and revoking all the embedded keys. The AAD 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. In addition, it is protected by the security mechanisms of the AAD; 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 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, guarantees that it cannot be tracked or identified by third-party devices, without the owner explicitly pairing them with the Nymi. For

more details on how tracking prevention and privacy are achieved by the Nymi, please refer to the "Cryptographic Protocols" section.

Privacy vs. Proximity

Proximity sensing is a feature of the Bluetooth 4.0 Low Energy standard. The transmitting device (the Nymi wristband) 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. While the proximity information reveals the presence of an electronic device, the Nymi broadcasts an encrypted signal that is decipherable only by its paired devices[20]. Any attempts to track the owner of the Nymi will fail because a third party device that was not paired with the Nymi will be receiving a signal that only contains random noise.

Conclusions

The Nymi was developed to improve the wearer's daily experience. 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 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 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 as an opportunity to create hyper-personalized solutions to their needs.

We are working to build a developer community that fosters creative energy. Our developer portal will be a platform for developers to voice their interests and work together to make their application ideas a reality. The developer community is a vital part of the Nymi ecosystem and we are excited to see how far people will push the technology.

As a team of eager engineers and scientists, Bionym aims to shape the world using novel concepts and technologies. Our brainchild, the Nymi, 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. 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.

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

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

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

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

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

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

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

13. Goldwasser, S., Micali, S. “Probabilistic encryption”. In Journal of Computer and System Sciences. 1984.

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

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

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

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

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

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

20. 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 user accesses (unlocks) their computer by gesturing their wristband.

Authentication

The process of assessing the Nymi user's identity by communicating their ECG wave to their AAD and companion app.

Authorized Authentication Device (AAD)

A smartphone, tablet, or computer that is compatible with Bionym's companion app. The companion app is developed for Android, IOS and PC; the user will need one of these devices to authenticate their Nymi wristband.

Biometric

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.

Companion app

Free software available for Android, IOS and PC that is required to enroll and authenticate a person's Nymi.

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 companion app when they first set up their Nymi wristband.

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 and a previous unknown pairing device (potential NED), 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 and an NED, and relays false messages in order to make the Nymi and the NED agree on an insecure key.

Nymi Enabled Device (NED):
Any device that is authorized to communicate with the Nymi – third party or Authorized Authentication Device.

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 communications and relays an identical message to a user's NED in order to access it without requiring their Nymi, 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 and a NED.

Spoofing

Recreating data to impersonate a communication. For Nymi user's, 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. For example 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.