Summary:

Personal Identifier the underlying methodology, is a discussion of the underlying methods delivering the death-knell to cybercrime enabled by leveraged credentials.

The Underlying Methodology:

The underpinnings of Personal Identifier are active acquisition of human trait knowledge used to determine the identity of the person in possession of the smartphone. While PI's collection and application of this knowledge is new, the concept of human trait acquisition by use of sensors is not. Several research projects over the recent past document the viability of using smartphone sensors to obtain reliable identifying information and characteristics of the person in possession of the device.

In practice, PI monitors a set of several traits. Three core traits are: device possession by a human; self-propelled motion; and location. These, combined with other physical, physiological, biometric, emotional, and behavioral traits of the person in possession represent the spectrum of candidate traits. Collectively, the set of monitored traits allow for accurate and reliable First User identification.

Within Personal Identifier there are two key perpetual processes, "learning" and "predicting".

The "learning" process monitors sensory inputs, detecting and recording trait patterns representative of the First User in possession of the device. A set of several different traits are in training at the same time. Learning occurs over several days following activation while the device is in the possession of the First User as they go about their normal daily routine. During this period, a baseline of knowledge representative of the First User's daily routine characterized by their traits is learned and recorded in a knowledgebase. Also, the list of traits is whittled down to a subset best suited for identification of this First User in recognition that not everyone has identical sets of traits useful for identification purpose. The dynamic process of selecting a subset of traits to monitor is necessary to reduce power consumption and performance demands. Doing so also delivers a level of security in that no one can know for sure what traits are being monitored. Thus, duplicating the traits becomes impossible. There is one such learning process per trait in the set being monitored and all remain active 24/7/365.

A knowledgebase contains computational artifacts of the learning process. Each stored artifact represents a single learning epoch for a single trait. On a per trait basis there may be thousands of such epochs each day, depending on the trait and the individual. The stored epoch artifacts represent the trait at an instant in time addressed by relative day and time of day. The period of the epoch is dependent on the trait and the person.

Following knowledgebase creation, learning shifts to "adaptive" mode. Adaptive learning detects nuances and deviations of the First User's traits leading to knowledgebase refinements. In effect, the knowledgebase becomes an active living thing by adapting changes in the lifestyle and environments of the First User. The concept of an adaptive living knowledgebase is diametrically opposed to that of the singularity of the statically stored password or biometric credential of present day authentication systems.

A "predictor" process monitors new sensory inputs, in effect comparing those with trait artifacts from the knowledgebase. The result is a three-state probability. The person in possession (1) is the First User or (2) is Not the First User or (3) is Indeterminate. This process occurs several thousand times per day, depending on the trait and the person in possession. The probability is produced by AI neural networks.

The third state, Indeterminate, triggers identity verification. A dynamic secret passcode query is derived on the instant and presented to the person in possession. This is in the form of a question for which there can be only one correct answer. The response is verified resulting in adjustments to predictor probability and knowledgebase. The secret passcode query is derived on the instant from the knowledge base and thus is something only the First User would know.

A "composite predictor" runs periodically or by query. It produces a composite probability of possession derived from all trait predictors. The probability is indicative of a First User in possession. Final determination is made by the inquisitor or by threshold registration settings. Application of the probability is application dependent.

Personal Identifier relies on use of Artificial Intelligence Neural Networks to accomplish its goals. The neural networks employed are specifically designed for the application of processing sensory signals in real-time. There are two such networks for each trait monitored and a third to implement the composite predictor. These specialized neural networks are tailored for low data density, high frequency real-time data sources.

With PI the gatekeeper requires only the First User's name or user name and cell phone number. Use of near proximity network for retrieval of Personal Identifier Code would add requirement to know that address too.

Personal Identifier provides active identification of a First User. It does so with none of the weaknesses of other types of credentials. It presents an impenetrable barrier to would be impersonators enabling immediate and automatic evasive measures on detection of impersonation attempts. As a smartphone App, cost of deployment is negligible. Additionally, its use is frictionless and it never needs maintenance as its basis is the active living knowledgebase that evolves with the First User's ever changing lifestyle.

Friction, or the lack thereof, is a crucial aspect of PI. Some might ask, so what's the big deal with entering a password, tap/swipe sequence, facial scan, finger print or other such identifier when accessing my phone? Where PI is concerned, this question is answered with a question. Why would you? Using PI, it is totally unnecessary. Pick up your phone, its ready to use.

Perhaps this short overview does not make clear that PI stores no Personal Identification Information either locally or remotely. The knowledge base consists of neural network artifacts. Even if made available to an outside party, unwinding these artifacts to their origins is impossible.

One caveat here is the dynamic password. In support of it PI does store the raw signal data for a selected trait. This data is stored internally with short time to live after which it is destroyed and replaced by a new set of raw sensory data taken from randomly selected traits.

Though not impossible to attack, the barriers presented by Personal Identifier are, from a practicality point, impossible to defeat.

Human Traits:

It's beyond the scope of this white paper to describe all human traits recognized by Personal Identifier. However, the following provide some examples.

Possession is an important trait. Knowing the device is in the actual possession of a human is a precursor to determining that person's identity.

Self-propulsion is a fundamental human trait reduced to step recognition. From this can be learned when the person typically walks and when they do not, the age of the person, the gender of the person and their mode of self-propulsion including walking, running or bicycling all learned from the physics of stride, pace, speed, direction and location. These same principals are also applied to the infirmed.

Applications:

In application the personal identifier methodology can be applied in every situation where credentials based authentication is now deployed. In many instances the cost of doing so is limited to a software upgrade.

Expanded use of automated identification using PI opportunities include physical access management and control such as vehicle, facilities, homes, campus and indeed any controlled access point. Event access management and secure area access management as well as presence recognition and detection are other applications that can benefit from us of PI.

Detractor:

It could be argued that not everyone has a smartphone, a valid point that in 2017 applied to about 30% of all Americans. As a counterpoint, nearly half of those are not online users and thus have no online accounts to protect. Of those left, it could be argued that from the savings realized by elimination of 43,000 cybercrimes each year, service limited smartphones could be provided to those without.

Further information on this and other security related interests and projects can be found at www.ProteqsIt.com.

Contact Information

Rick Hallock
Rick.Hallock@ProteqsIt.COM
Phone: (239) 370-0246

Resources and Works Cited