Summary:

Did you know? 50% of all cyberattacks in 2014 were leveraged by stolen or weak credentials. It grew to 63% in 2015. 2016 was a banner year at an astounding 81% [1]. In 2017, sizing the piece of the pie is no longer relevant, we experienced over 43,000 successful accesses using stolen credentials.

The trend is obvious and the velocity scary, but it doesn't have to be that way.

In this paper I discuss the merits and methods of "Personal Identifier", a patented methodology developed over a five year period that addresses the core issue enabling the rapid rise in cybercrimes enabled by leveraged credentials.

Background:

Cyberattacks enabled by leveraged credentials begin with an undetected impersonation attack. The impersonation attack is made possible by theft of identity. The stolen identity equips the cybercriminal with the much sought after identification credentials. Once in possession the cybercriminal has nothing more to do than present the credentials for authentication after which they are granted access. The takeaway is this: given the impossibility of keeping credentials secure implies there is no amount of tweaking the current identification model to solve this problem while continuing to rely on the credential.

The Problem

Credentials based authentication depends on user identification by use of credentials provided by an unseen, unknown person and at a distance. And therein lies the problem; "any unknown person" can present the credentials of another. The authenticator recognizing a valid credential admits the "unknown presenter" without further consideration.

Stated simply, credentials based identification and authentication has never worked and never will. No matter how many times the basis of the credential are enhanced the core problem remains. The password and the PIN are failures, the phrase as a password is no better, the finger print, palm print and facial recognition are failures. Multi-factor authentication suggests a solution that is based on presentation of two or more defective credentials.

Solution:

Resolving the failings of present day identification methodologies requires thinking outside the box. Doing so with an understanding of present attack vectors at the core of the problem.

Personal Identifier (PI) methodology adopts "active identification". It does so by actively monitoring the identity of the person in actual possession of an identification device on a 24/7/365 basis. Identification is facilitated by learning the human traits of the person assigned the device, the First User. Then, by monitoring those human traits of the person in possession it becomes possible to detect if that person is the First User.

The smartphone is an ideal identification device. It's ubiquitous and used by over 250 million Americans. It is unique on a worldwide basis. It's identifier, the phone number, offers little risk of personal identification information loss even if harvested. It has response channel options of Bluetooth, WiFi and observable bar or QR code, each of which is uniquely identifiable. It is the ideal vehicle for hosting the Personal Identifier methodology. The perfect personal identification device applicable in most authentication scenarios.

To identify and authenticate someone seeking access a gatekeeper transmits an identification query with session identifier over cellular network to the First User's smartphone. Upon receipt, a probability of possession by First User is produced. A token, the Personal Identification Code is created containing that probability, the session identifier and the internal smartphone identifiers. That token is transmitted in response to the query by any of several methods, be it over cellular, Bluetooth or Wi-Fi network or by bar or QR code display. The entire transaction takes a fraction of a second without user friction. The gatekeeper receives and validates each of the token components: is the session identifier and its latency valid; is it from the expected device belonging to the First User's; and at that instant in time is the smartphone in the actual possession of the First User. If all valid, grant access, otherwise deny access.

Human traits, the key to the methodology, are unique. Human traits can be detected using sensory circuits of a smartphone. Sensory inputs can be learned by use of Artificial Intelligence neural networks using machine learning methods. The learned traits of a person uniquely identify that person and only that person from all others on earth. The possibility of impersonating a random set of human traits is, from a practical standpoint, impossible. Especially so given the traits used are randomly selected and known even to the person they represent.

Personal Identifier traits based identification as described above addresses each of the perfect solution needs:

- A smartphone is unique on a worldwide basis, it cannot be replicated.
- The authentication site has no need for stored credential or PII. Statically stored is user name, cell phone number, and device identifiers.
- Human traits are unique, unknowable and not reproducible.
- Active production of possession status by adaptive human trait recognition insure the impossibility of impersonation.
- Dynamic pass codes assure possession by a specific person.
- Multi-channel process precludes man-in-the-middle attack.
- Use of internal device identifiers negate risk of account hijacking.
- Absolutely no friction.
- Adaptive learning insure up-to-date human trait status and knowledge.

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 Personal Identifier 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 Personal Identifier.

A favorite example applicable to the times is campus-wide security. Securing a campus is, in part, the need of knowing who is attempting to enter or leave the campus setting and where they are if present on campus. With the assumption that every person authorized to be on campus has a Personal Identifier enable smartphone then campus security staff have a new and very powerful informational tool at their disposal. With it, security is informed of each and every person entering the campus. They are likewise informed of all persons leaving campus. And most important of all, they

know when someone who does not belong is entering. A well deployed Personal Identifier monitoring system would also give security the benefit of knowing exactly where each person was while on campus.

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

[1] http://www.VerizonEnterprise.com, Verizon 2017 Data Breach Investigations Report. Retrieved September 18, 2017.

[2] http://www.VerizonEnterprise.com, Verizon 2016 Data Breach Investigations Report. Retrieved July 12, 2016.

[3] http://www.VerizonEnterprise.com, Verizon 2015 Data Breach Investigations Report. Retrieved July 12, 2016.

[4] Atallah, L., Yang, G.Z. The use of pervasive sensing for behavior profiling—a survey. Pervasive Mobile Computing. 5(2009), 447–464.

[5] Neil Johnson, David Hogg. Representation and synthesis of behavior using Gaussian mixtures.
20(12), 889–894, 2002.

[6] C. McCool, S. Marcel, A. Hadid, M. Pietikainen, P. Matejka, J. Cernocky, N. Poh, J. Kittler, A. Larcher, C. Levy, D. Matrouf, J. Bonastre, P. Tresadern and T. Cootes. Bi-Modal Person Recognition on a Mobile Phone: using mobile phone data. Proc. Multimedia and Expo Workshops, 635-640, 2012.

[7] E. Miluzzo, A. Varshavsky, S. Balakrishnan, R. Choudhury. TapPrints: Your Finger Taps Have
Fingerprints. Proc. Mobile Systems, applications and services, 2012.

[8] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, Heinrich Hussmann. Touch me once and I know it's you! Implicit authentication based on touch screen patterns. CHI, 987-997, 2012.

[9] Sumit Shekhar, Vishal M. Patel, Nasser M. Nasrabadi, Rama Chellappa. Joint Sparse
Representation for Robust Multimodal Biometrics Recognition. IEEE PAMI. 36(1), 113-126, 2014.

[10] Kwapisz, J.R., Weiss, G.M., and Moore, S.A. Cell phone-based biometric identification. Biometrics, 2010.

[11] Wolff, Matt. Behavioral Biometric Identification on Mobile Devices. Foundations of Augmented Cognition. Springer Berlin Heidelberg, 783-791, 2013.

[12] http://www.VerizonEnterprise.com, Verizon 2018 Data Breach Investigations Report. Retrieved June 18, 2018.