Summary:

Did you know? In 2014 50% of all cyber attacks were leveraged by compromised credentials. It grew to 63% in 2015 and 2016 saw a banner year with an astounding 81% [1]. In 2017, reporting the statistic as a percentage of the cybercrime pie is no longer relevant given there were over 43,000 successful cyber attacks leveraged by compromised user credentials.

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

In this paper, we discuss the merits and methods of "Personal Identifier," an identification methodology that puts the "human" in the process of identifying humans.

Background:

Since the inception of the Internet and its username and password security measures we have lived with identity theft leading to impersonation attacks. Based on the premise that if presented credentials are valid, then it's okay to "assume" the person presenting them is the person they belong too. In it's simplest form, if a person seeking access could present valid username and password, then access was "assumed." No wonder Verizon researchers [12] uncovered over 43,000 successful cyber attacks in 2017, all leveraged by use of stolen identities. The flawed method of human identification based on a credential and "assumed" identity put out the welcome mat to cyber attackers who take full advantage of it. Juxtapose that reality with another, the recognition there have been no airline hijackings in America since the inception of the TSA security check-in procedures. Why is that? Could it be inclusion of a human in the process of identifying humans?

It's a fact that no past, present or future identification process based on credentials alone will succeed in reducing these astounding statistics for the simple reason that all accept the "assumption" of identity. Those SFA and MFA solutions that require human interaction such as USB and NFC security keys and a few smartphone Apps include a human, any human, in the identification process. Sadly all accepting activation from any human, even the cyber attacker, leaves in place the "assumption" of identity underpinning of a flawed methodology.

Solution:

This problem and its solution seem obvious; why must we continue reliance on the vagaries of credentials based identification and forced assumption of identity? Why not focus on identifying the individual without the use of a credential and without the "assumption" of identity? Doing so eliminates the argh moment when mistyping the password, PIN or second-factor one-time password. Never again struggle to remember the complex password or to find the required password amongst many. Avoid the frustrations of taking multiple facial image shots to get one that's just right and acceptable to the device or having fingerprint recognition fail because of less than a perfectly clean thumb. And the elephant in the room, the methodology that by its very design promotes impersonation attacks. Imagine a world in which there are no phishing attacks and in which the value of Personal Identification Information is substantially reduced by its no longer containing credentials related information, perhaps to the point where we no longer read of PII harvesting of millions and in one reported case BILLIONS of records.

Personal Identifier foresees a world such as this, a world in which credentials are relegated to the dustbin of technology history and replaced by a focus on identifying the human and doing so without the use of credentials.

Personal Identifier (PId) includes the human in the process by "active identification" methods. A smartphone with Personal Identifier App actively monitors the identity of the person in possession on a 24/7/365 basis. During a training period, it learns the human traits of its principal, the person to whom the device is assigned. And then, by actively monitoring those same human traits of the person in possession, it recognizes that person's identity as being or not being the principal. Thus, by a query sent the PId smartphone device response is received that includes a secure identity token indicating device possession status at the instant of the query. Possession by a human indication eliminates the potential of impersonation by a bot. If in possession of a human then identity provided indicates if by principal thus eliminating the risk of impersonation by someone other than the principal.

In sum, assured identification of the person in possession of the PId device without risk of impersonation by another person or a bot.

The smartphone is an ideal PId platform device. It's ubiquitous and used by over 250 million Americans. It is unique on a worldwide basis. It's identifier, the phone number, poses minimal risk of personal identification information leakage, even if harvested. It has query and response channel options of

Cellular Network, Bluetooth, WiFi, and observable bar or QR code. It is the ideal vehicle for hosting PId and is already an accepted device and integral part of many the identification process.

In a familiar login scenario using PId in place of username and password, the gatekeeper transmits an identification query to the principal's smartphone. The smartphone PId App responds by producing and returning a probability of possession token to the gatekeeper. The gatekeeper validates the probability of possession token, and grants access if and only if the person in possession of the smartphone is its principal. There is no opportunity for impersonation by another person or a bot.

Human traits, the key to the Personal Identifier methodology, are unique. Human traits are detected using sensory circuits of the smartphone. Artificial Intelligence machine learning techniques are employed to learn the human traits of the device principal. They uniquely identify the principal from all others on earth.

A set of human traits best suited for recognition of the principal are dynamically selected from a library of several candidate traits. Those selected are known only to the PId App and only at runtime. It’s impractical for the cyber attacker to discover the traits monitored for a given principal. Even if done, consider the problem faced by a potential attacker in mimicking those traits. Consider for example the simple trait of walking. Sounds simple but the attacker must master the principals fluid steps when walking down a hallway as well as the sporadic steps occurring when working in the kitchen and on to those pesky steps occurring during the principal's power walk. The wannabe attacker must then factor in the time of day, the day of week when steps occur as well as both geophysical and RFI environmental locations of where they occur. All-in-all, an impossible feat.

The step trait is but one example of the complexities facing anyone attempting to impersonate the PId principal. Simply put, it is impossible to do so.

A few benefits of Personal Identifier include:

- A PId enabled smartphone is unique on a worldwide basis; replication is impossible.
- There are no stored credentials or Personal Identification Information.
- Human traits are unique, unknowable and impossible to reproduce.

- The principals monitored human traits are selected at random and learned as an automated machine learning process.
- Active production of possession status at time of query.
- Adaptive recognition of human trait changes applied to freshen the traits knowledge base on an as-needed basis.
- Multi-channel access impedes man-in-the-middle attacks.
- Use of internal device identifiers prevent account hijacking.
- Frictionless during use and minimal friction when registering.

Applications:

Personal Identifier is applicable in every situation where credentials based SFA or MFA authentication are now employed. In most instances, the cost of doing so is limited to a software upgrade.

Retaining present SFA or MFA methodologies with the added benefits only Personal Identifier can provide is possible can reduce the cost of adoption even further.

Automated identification using Personal Identifier opportunities include physical access management and control such as for vehicles, facilities, homes, campus and indeed any controlled access point. Presence awareness access management can be achieved using Personal Identifier. Indeed, the number of applications for which Personal Identifier is too numerous to address here in a white paper brief.

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.