NOPASSWORD™

WHY NOPASSWORD?

https://www2.nopassword.com

☎ +1 877-877-5587

WHAT IS NOPASSWORD

NoPassword is the next generation of identity and access management that substitutes passwords with H^{2}MFA^{TM}. Every time a user needs to be authenticated - for instance to access their account - they will get authenticated locally on their smartphone (or other authentication devices) based on their biometric. Then, NoPassword extracts some hidden features from the user's phone and uses the PKI to authenticate the user's phone with the authentication server to give the user access to their account.

NoPassword is a FIDO UAF certified solution that goes beyond FIDO requirements and even PKI to make sure the authentication is processed securely and privately. NoPassword does NOT store Personally Identifiable Information (PII), such as user's biometric or passwords, on its authentication server or any centralized database. Instead, it securely and privately stores and leverages mathematical representations of user's biometric on the user's smartphone. This information is not transferred between devices nor is it accessible by applications and other businesses.

WHY IT'S TIME TO GO NOPASSWORD

In the past, there have been four barriers that limited the widespread use of biometric solutions. These four barriers included: 1) acceptable level of security and convenience of conventional solutions (i.e. passwords and second factors); 2) lack of availability of biometric sensors on different devices and high cost associated with leveraging biometrics; 3) privacy and security concerns around storing users' biometric information on a centralized database; and 4) complexity of integrating biometric solutions.

Today, the ineffectiveness of conventional authentication solutions along with the technological advancements and widespread availability of biometric sensors have lead to overcoming first two barriers of widely used biometric solutions. On the other hand, NoPassword offers a solution that eliminates the need of a centralized PII database (including stored biometric information) by adding hidden multi-factor authentication on top of human factor (biometric). Consequently, NoPassword leverages biometric authentication securely and privately, and enables quick and easy integration with existing enterprise resources and solutions. As a result, the NoPassword portfolio of products and recent technological biometric advancements together overcome all the previous barriers and it is changing the paradigm of identity and access management.

This document will further expand on the security and inconvenience concerns around conventional solutions - such as passwords and second factors. Then, it demonstrates why NoPassword focuses on authentication on smartphones: as 1) smartphones are becoming widely adopted by consumers, 2) smartphone security improves, and 3) biometric sensors (such as fingerprint readers, cameras, and microphones) are widespread on smartphones. It also expands on the changing attitude of consumers on the use of biometrics. It will highlight how the NoPassword solution improves security while maintaining privacy of users. Lastly, it briefs how NoPassword provides integration tools and resources to quickly and easily implement its solution and enable you to bring a no password experience to your workforce and customers - allowing you to modernize your stakeholders identity today.

CONVENTIONAL AUTHENTICATION SOLUTION ARE INADEQUATE

Conventional authentication solutions (i.e. passwords and second factors) are no longer able to address our needs. Their incompetences can be broken into two categories: security and inconvenience.

THE SECURITY CHALLENGES

Verizon[1] Data Breach Investigation Report states that over 85% of cyber attacks in 2015 were carried through stolen credentials, key loggers, social engineering and phishing - all targeting passwords. Recent identity breaches (e.g. LinkedIn, Yahoo, Experian, DropBox) compromising billions of users' accounts and passwords are evidences that passwords are not up to the task any more.

Some companies and businesses have started to use some security policies such as complex password practices and password rotation policies, and security questions to tackle the cyber security threats. However, these policies have proven to be ineffective as the National Institute of Standard and Technology (NIST) advices enterprises to be mindful of the fact that most of these policies drive the users to turn into insecure practices[2].

Other businesses have implemented a variety of second factors that not only create tremendous inconvenience but have also been proven ineffective. Recent vulnerabilities of Gmail accounts secured by Google authenticator[3] and Facebook account[4] are some examples. Man-in-the-middle, man-in-the-browser, man-in-the-mobiles, and specifically, spy agents are some of the most common attacks that conventional second factors, OTPs, and SMS based 2nd factors are not able to provide protection. NIST recent Digital Authentication Guideline highlights 2nd factor authentication challenges, specifically discouraging the use of SMS based 2nd factors[5]. Following NIST recommendations, all US Federal Government agencies are now required to adopt other authentication methods and private organizations also need to take NIST recommendations serious. Bear in mind, these cyber attacks have been extremely costly for every organization including the private sector.

Kaspesky Lab estimates the direct costs of data breaches to be $551,000 for every 1,000 employees and if an attack results in service interruption, on average it costs $1.4 million[6]. Other research estimates that on average, cyber attacks cost every enterprise $3.5 million per year[7]. The damage to the enterprise brand is estimated to be 7.5 times higher than direct and recovering costs presented above[8]. Lost revenue and decline in returning business as a result of customers not ailing to trust the business is considered to be the most costly damage of every cyber attack. While total cost of cyber attacks in 2014 and 2015 were respectively estimated $400 billion[9] and $500 billion[10], this numbers is expected to significantly grow in the following years to reach over $2.1 Trillion by 2019[11].

THE INCONVENIENCE CHALLENGES

With the proliferation of smartphones and online applications, the average user has over 150 unique accounts and corresponding credentials. A large proportion of users use one password for multiple accounts and when they are forced to regularly change their password or use complex passwords, they either turn to insecure practices or regularly have trouble remembering their passwords.

Failure to remember passwords for customers means service interruption, user frustration, and brand impact. In some cases, companies report that this results in lost revenue due to missed engagement or failure to register new users who require to setup an account with a strong password, especially when it comes to using mobile device and requiring to enter or setup password on small screens (e.g. mobile phones screen).

Getting locked out as a result of forgetting password or missing the periodic deadline to rotate password is a common experience for employees who face password rotation policies. These incidents are more common in organizations where staff are not allowed to reuse previous password and are required to setup complex passwords. This not only creates user frustration and lower productivity but also increases IT costs and wasted resources.

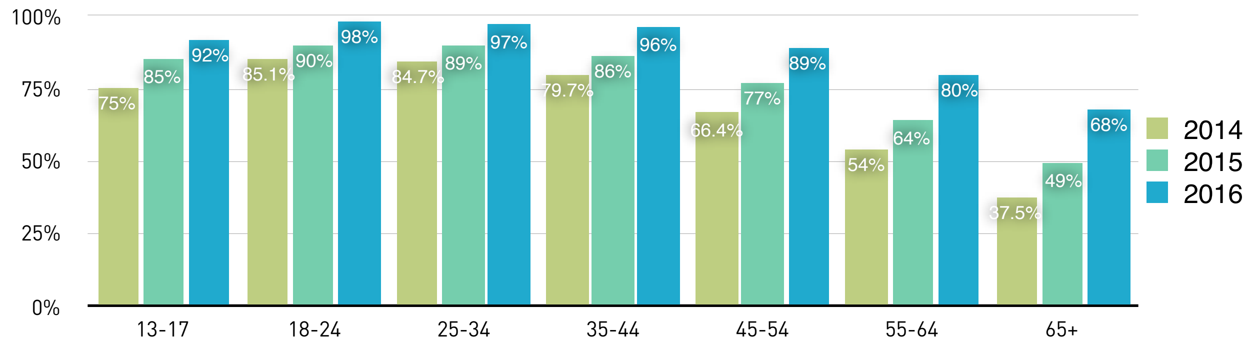
Besides, second factors - such as dongles, OTP tokens, and smart cards - are well-known for creating additional frictions and inconvenience. These are the reasons why they have not been widely implemented. Normally implementing second factor follows by users' complaints and dissatisfaction which leads IT departments to limit the use of second factors to a few very sensitive applications. With an increasing number of employees who use multiple devices and/or their phones and tablets for work, the challenge of using second factors, specially smart cards, is becoming more problematic.

SMARTPHONE DOMINANCE

Smartphones are widely available and they are becoming even more popular due to their technological advancement and falling cost. 88% of US population own smartphones in third-quarter 2016. This number has grown by eight points from the same time last year (from 80% in third-quarter 2015) and expected to grow to 92.8% by 2020 - which means by 2020, over 92% of US population will own a smartphone, making them a perfect candidate for authentication purposes[12].

Nearly all millennials and younger US generation are smartphone users: 98% of 18 to 24 year olds, 97% of 25 to 34 year olds, 96% of 35 to 44 year olds own a smartphone in 2016[13]. Although this number is lower amongst older generations; smartphone penetration has had the highest growth among the older generation. Several market research have predicted the smartphone adoption is going to grow among the older generation[14], and even lower income individuals[15]. This trend becomes more obvious, especially if we compare smartphone penetration amongst older generation in last three years as shown in the following chart. In the past two years, the older generation (65+) grew from 37.5% to 68% and it's expected to continue to grow.

Smartphone Penetration by Age (US)



Source: comScore (2015) and The Nielsen Company (2016)

This trend is not unique to the US. Similar growth in smartphone adoptions by different demographic are reported in other countries; both developed and developing countries[16]. While, the speed of smartphone adoption had been faster in developed counties. Availabilities of cheaper smartphones and older version with lower prices has accelerated growth in smartphone ownership in developing accounts in the past two years.

ADVANCEMENT IN SMARTPHONE SECURITY

Mobile device technology has come a long way. Specifically, both iOS and Android operating systems include secure elements. Nearly all, over 99% of smartphone, are either iOS or Android operating systems[17]. iOS operating systems include "Secure Element and Secure Enclave that are a tamper-resistant platform capable of securely hosting application's confidential information, cryptography keys with the rules and security requirement set forth by a set of well-defined trusted authorities"[18]. On Android operating system, Trusted Execution Environment (TEE) -secure area of the main processor in a smart phone (or any connected device). It ensures that sensitive data is stored, processed and protected in an isolated, trusted environment. The TEE's ability to offer isolated safe execution of authorized security software, known as 'trusted applications', enables it to provide end-to-end security by enforcing protected execution of authenticated code, confidentiality, authenticity, privacy, system integrity and data access rights. Comparative to other security environments on the device, the TEE also offers high processing speeds and a large amount of accessible memory"[19]. Along with Secure Element and TEE, NoPassword also uses white box technology to isolate sensitive information such as biometric templates and cryptographic keys and run its application in a secure environment. All this advancement turns smartphones to the best platform for authentication purposes".

BIOMETRIC SENSORS ON SMARTPHONES ARE NOW MAINSTREAM

Recent technological advancements in biometric sensors and cameras have enabled smartphones to be the best and most available biometric authentication platform. According to a new market research report, because of these advancement, the biometric system market size is expected to increase from $10.74 Billion in 2015 to $32.73 Billion by 2022, at a CAGR of 16.79% between 2015 and 2022[20].

Over 28% of the global base of smartphones in use are equipped by fingerprint sensors. The number of smartphones models featuring biometric capabilities rose from 52 to 197 over the last year[21]. This growth is due to dropping prices - average price of such smartphones have decreased from $800 in 2013 to $250 in 2016. New reports also reaffirm that by the year 2018, biometric technology (mainly fingerprint) will be on 100 percent of smartphones[22]. On the other hand, 100% of smartphones are equipped with quality front-cameras and microphones that can be utilized for face and voice authentication. Therefore, biometric sensor technology on smartphones are becoming "officially mainstream" in the US.

CONSUMER ACCEPTANCE OF BIOMETRIC TECHNOLOGY

Additionally, consumers' awareness and acceptance of biometrics technology have changed. While biometric capability technologies have significantly improved and adopted widely, people are even more comfortable using it and trust that their information is secured. According to the Consumer Technology Association (CTA) report, Biometric Technologies: Understanding Consumer Sentiments, "A large percentage of U.S. … adults are comfortable with biometric technologies being used at places perceived as highly secure (airports) or in need of greater protection. U.S. adults view entities that currently handle (sensitive) personal information securely such as health care organizations and banks more favorably with managing biometric information"[23].

This is not limited to the U.S. Most adults in the UK, for example, are now willing to embrace biometric identity for online banking. When it comes to managing accounts online, three in five people (61%) believe biometric identification is either just as secure, or more secure, than the current system of passwords[24]. UK adults are far more comfortable using biometric technology to access their online banking than their social media accounts – twice as much, 64% compared 32%[25].

NOPASSWORD - PRIVACY AND SECURITY BY DESIGN

NoPassword as a pioneer in implementing biometrics in identity and access management and is dedicated to provide the most secure and private solution to financial institutions, healthcare and insurance institutions, and other industries. The NoPassword solution has integrated biometric authentication (e.g. face, voice, fingerprint, smart pattern) methods with a maximum False Acceptance Rate of 0.002%[26]. NoPassword is designed to secure users' biometrics on their smartphones and have them under the user's control to enhance privacy and security. NoPassword has implemented a proprietary technology and the best in class encryption technology to secure user's PII, especially biometrics on their smartphones and uses hidden features of the phone to enhance the authentication process and user experience. This will eliminate the need of a centralized PII database. Therefore, the large scale attacks that would result in the loss of large numbers of users' passwords, credentials' or biometrics would be irrelevant.

With NoPassword, every business would be able to prevent the main portion of costly cyber attacks, ensure users and employees privacy, and deliver the ease of use and immediate access to their stakeholders. With NoPassword, you no longer need to worry about stolen credentials, phishing, social engineering, and key logger attacks. Imagine your IT no longer handling password reset requests and only focusing on the providing the best service to your stockholders. NoPassword complies with regulatory compliance of financial, banking, healthcare, and insurance industries.

EASY INTEGRATION OF NOPASSWORD WITH EVERYTHING

One of the biggest challenges of a password-free and biometric solution has always been costly implementation and complex integration with existing solutions. NoPassword offers quick on-cloud and on-premise deployment based on your needs. Wide range of integrations with your existing enterprise resources (such as single sign-on, Rest API, OAuth, OpenID, AD, CAS, Radius, and LDAP), allows you to quickly and easily integrate NoPassword for all applications used by your workforce and customers. With a large number of applications pre-integrated and cataloged, you spend less time on integrations and more time focusing on your core objectives. There is no need to tear down or replace any solution that you are currently using and happy with it. NoPassword can simply sit on top of your existing infrastructure to bring a password-free experience to your stakeholders.

REFERENCES

[1] Verizon (2016) Data Breach Investigations Report: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[2] NIST (2016), DRAFT Guide to Enterprise Password Management: http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

[3] https://citizenlab.org/2015/08/iran_two_factor_phishing/

[4] http://www.forbes.com/sites/thomasbrewster/2016/06/15/hackers-steal-facebook-account-ss7/#27bcdf148fa7

[5] NIST (2016), Digital Authentication Guideline, Authentication and Lifecycle Management: https://pages.nist.gov/800-63-3/sp800-63b.html

[6] Kaspersky Lab (2016), The True Costs of a Cyberattack for Enterprises: https://business.kaspersky.com/cost-cyberattack-enterprise/5195/

[7] http://www.businesswire.com/news/home/20160718005304/en/Ponemon-Institute-External-Cyber-Attacks-Cost-Enterprises

[8] Kaspersky Lab (2016), The True Costs of a Cyberattack for Enterprises: https://business.kaspersky.com/cost-cyberattack-enterprise/5195/

[9] Lloyds (2015), cyber crime cost businesses up to $400 Billion a year: http://www.cyberinsurance.co.uk/cybernews/lloyds-ceo-cyber-crime-cost-businesses-up-to-400-billion-a-year/

[10] http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#620cc5983bb0

[11] Juniper Research (2015), CYBERCRIME WILL COST BUSINESSES OVER $2 TRILLION BY 2019: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

[12] The Nielsen Company (2016), "Millennials Are Top Smartphone Users," www.nielsen.com/us/en/insights/news/2016/millennials-are-top-smartphone-users.html

[13] The Nielsen Company (2016), "Millennials Are Top Smartphone Users," www.nielsen.com/us/en/insights/news/2016/millennials-are-top-smartphone-users.html

[14] BI Intelligence (2012): http://www.businessinsider.com/us-smartphone-market-2012-9

[15] PewResearch (2015), US Smartphone Use In: http://www.pewinternet.org/2015/04/01/chapter-one-a-portrait-of-smartphone-ownership/

[16] Pew Research Center (2016) "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies," http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/

[17] Gartner Newsroom (2016) Press Release: "Five of Top 10 Worldwide Mobile Phone Vendors Increased Sales in Second Quarter of 2016," http://www.gartner.com/newsroom/id/3415117

[18] GlobalPlatform Whitepaper: "GlobalPlatform made simple guide: Secure Element," http://www.globalplatform.org/mediaguideSE.asp

[19] GlobalPlatform Whitepaper: "GlobalPlatform made simple guide: Trusted Execution Environment (TEE) Guide", http://www.globalplatform.org/mediaguidetee.asp

[20] Markets and Markets (2016), "Biometric System Market by Authentication Type (Single-Factor: (Fingerprint, IRIS, Palm Print, Face, Vein, Signature, Voice), Multi-Factor), Component (Hardware and Software), Function (Contact and Non-contact), Application, and Region - Global Forecast to 2022," http://www.marketsandmarkets.com/PressReleases/biometric-technologies.asp

[21] MobileIDWorld (2016), "Smartphone Biometrics Are Officially Mainstream: Acuity," http://mobileidworld.com/smartphone-biometrics-are-officially-mainstream-acuity-102124/ AND Acuity Market Intelligence (2016), "Market Research - Biometric Smartphone Model List," http://www.acuity-mi.com/BSP.php

[22] Biometrics Research Group (2016) "Mobile Biometrics Market Analysis," http://www.biometricupdate.com/wp-content/uploads/2015/10/287127021-Mobile-Biometrics-Market-Analysis-5.pdf AND FindBiometrics Global Identity Management (2016), "All Smartphones Shipped In 2018 Will Feature Biometric Tech: Acuity," http://findbiometrics.com/smartphones-biometric-tech-acuity-307221/

[23] Consumer Technology Association (2016) "Biometric Technologies: Understanding Consumer Sentiments," https://www.cta.tech/News/Press-Releases/2016/March/Biometric-Technology-Enjoys-Strong-Support-from-Co.aspx

[24] International Biometrics + Identity Association (2016), "Public Perceptions of Biometrics," https://www.ibia.org/download/datasets/3372/Public-Perceptions-of-Biometrics-opinion-surveys%20.pdf

[25] Experian (2016), "UK now ready for biometric banking" https://www.experianplc.com/media/news/2016/uk-now-ready-for-biometric-banking/

[26] NoPassword Human and Hidden Multi-Factor authentication include two parts. The first part is the human or biometric authentication, which takes advantage of fingerprint, face, and voice authentication. All the biometric authentication implemented in NoPassword solution has a False Acceptance Rate of no more than 0.002%. This means there is a chance of finding 1 false match to a user biometric for every 50,000 user's biometric that is tried. Since NoPassword takes advantage of hidden multi-factors extracted from the user's phone and each user's biometric is secured on their own phone, it is impossible to use another phone other than a user's phone to access their account. The number of false attempts on each smartphone is limited to (3,5, or 9), and therefore there is no chance to try a large number of biometrics on a single device. Combining all these elements, the false acceptance rate for NoPassword solution is practically zero. Please refer to the NoPassword security white paper to find out more on the security of NoPassword biometric authentication.