Usable Security - Identity and Authentication

Reducing Friction in Security

Technology Landscape Briefs

Author:
Vivek Srivastav
SrVP Research and Innovation, ReBIT

Date: Sept 2018

Abstract: Will there always be a tradeoff between security and convenience or some of the new emerging technologies offer a respite from these tradeoff and improve both the convenience as well as security of the system? This whitepaper explains some of the nuances between identity, authentication and authorizations and discusses some emerging technologies and trends that have potentials to improve security without compromising user experience.

Disclaimer: *The mechanisms suggested in the document are indicative. There may be alternative ways to achieve the same objectives. Organizations may consult experts and implement a strategy most suited and aligned with their own organizational objectives.*

1. Usable Security **2**
1.1. Authentication vs. Identity 2
1.2. Security and Usability 3
2. Authentication and Authenticators **3**
3. Identity **6**
4. Way Ahead **7**
5. Terms used/coined in the article **8**
6. Reference **9**

1. Usable Security

Recently DSCI organized a panel discussion on “new age authentication technologies” in their FinSec Conclave 2018. Several sessions in RSA Conference 2018 covered the topic of digital identity and authentication. Many new innovation are looking at the topic on biometric and AI driven authentication such as the FIDO alliance and some startups companies (Smokescreen, Sparsha & NeoEyed). Furthermore, NIST special publication 800-63 presents some original thoughts in the area of digital identity and authentication. The identity and authentication is an important topic in cyber security discussions.

There has always been a tussle between security and convenience and many have argued in past that it is a tradeoff between the two. Will there always be a tradeoff or some of these new emerging technologies offer a respite from these tradeoff and improve both the convenience as well as security of the system? Is it possible to improve security without increasing friction in validating the user?

This whitepaper explains some of the nuances between identity, authentication and authorizations and discusses some emerging trends that have potentials to improve security without compromising user experience.

1.1. Authentication vs. Identity

The identity is a set of claimed attributes and authentication is a mechanism to verify a set of claimed attributes. The article describes some of the recent advances that have happened in the field of identity and authentication, specifically how the identity and authentication landscape is changing and how it has potential to improve both security and users’ experience.

1.2. Security and Usability

Security and Usability have always been thought to be at odds with each other. While the security engineers have always seen the friction as a necessary means to prevent and protect the system and the users; the e-commerce and monetary transactions has always found diminished returns in increased friction. Security requires interplay of people, process and technology. All the three should be aligned for effective security. For example, the poor usability experience has prompted users to find ways to circumvent security controls. Don Norman In his book “The Design of Everyday Things”, gives an example of how the nurses circumvented the auto-lock feature because the auto-lock feature enabled for privacy and security interfered with the normal operation of their activities. The cognitive burden imposed by complex passwords requirements has prompted people to reuse passwords across multiple applications. Storing the passwords in files, sharing of password by multiple people has been found in many instances. Although, in several instances the single factor authentication has given ways to multi factor authentication mechanisms that uses two or more modes of “what you know”, “what you have” and “what you are” authenticators to authorize a user, there is still a need to further strengthen the authentication mechanisms that doesn’t

compromise on user experience. The memorized tokens used for establishing "what you have" may have outlived its usefulness as we have come to age of almost daily reporting of some data breaches. The modern advances may even have the potential to enable **invisible security with zero friction** and promises better identity verifications and authentication as compared to present prevalent mechanisms.

2. Authentication and Authenticators

Memorized tokens: One might expect that a complex password policy such as asking users to use a combination of small and upper case letters, numbers and symbols would provide for a better security but research in this area points out that this prompts people to simplify the password and then reuse them over and over. Use of password analysis tools such as hashcat has shown that a great percentages of users use predictable password. In fact, NIST in its special publication recommends the following:

- Remove all password complexity rules, they create a false sense of security. Instead check and forbid use of commonly used password.
- Remove need to reset password periodically, instead throttle and limit number of password retries.
- Enable show password when typing
- Allow paste in password field

These recommendations underscores the importance of usability in security design.

The memorized tokens represents an old school antiquated mechanism to authenticate users. In the age of data breaches (yahoo, equifax, LinkedIn) , users maintaining upwards of 40+ accounts, and varying levels of salting and hashing security employed might expose users to compromises if memorized tokens are the only way of authenticating the user to a system. Tory Hunt, on his website https://haveibeenpwned.com/ maintains information about more than 5 billion accounts that have been pwned in data breaches. Recent t-mobile Australia inadvertent disclosure by a support personal that they store passwords in clear text is an example of how weaker security in one website once breached and compromised might expose a user to another website when user ID and passwords are reused. The advent of AI and ML further adds to hackers tools arsenal for analyzing breached data and poses threat to memorized tokens.

Studies on challenges related to memorized tokens
• In 2016, Experian found that millennials had on average 40 services registered to a single email account, and only five distinct passwords. • A 2010 study by Weir et al. found that users will simply capitalize the first letter of their password and add a "1" or "!" to the end, making the password no harder to crack. Any password cracker worth their salt knows about these patterns and has adjusted their tools accordingly. • When required to use numbers in their passwords, a full 70% of users on rockyou.com (which contained user info for several social networking sites) just added numbers before or after their password.

Lookup and OTP tokens: In contrast to the memorized tokens "what you know" mechanisms, "what you have" mechanisms provide some assurance against data breaches. RSA tokens generators, Google Authenticators, Grid based authentication, and other OTP based mechanisms are examples of such "what you have" authentication mechanisms. Typically implemented in addition to the memorized tokens, these authenticators provide better resilience when MFA is enabled in the system. Arguments to enable MFA on all systems have been made. While MFA adds an additional layer of assurance, it does create friction in the authentication process. Some systems use adaptive authentication mechanisms to reduce friction and improve assurance such as when changes are detected in users' environment additional authentication factors are dynamically introduced.

There are some **in-band authenticators** which may directly interact and perform authentication with the user out of band on a secondary channel such as an IVR, a web link etc and based on it authorize the user over the primary access channel. Whereas some common type of **out-of-band authenticator** will deliver a OTP code over a secondary channel, that is then submitted through by the user over the primary channel for authentication. This 'out-of-band authenticator' mechanism is used for authorizing the financial CNP transactions in India.

Vulnerabilities in "What you have" authenticators
• SS7 protocol vulnerabilities • SIM cloning • Email hacking

Some technology advancement have happened in "what you have" authenticator mechanisms, specifically the use of device binding and other device characterization, detection based on geolocation and analytics. These mechanisms strengthens the "what you have" authenticator process, but continue to cause friction in users interactions. Furthermore, some of these authenticators face security concerns specifically on mobile platforms and our reliance on emails as a means to identity our identity (see the table above).

Mr. Lalwani from Saparsa adds that as smartphones have become the ubiquitous form of commerce especially in India, the "what you have" is not always the most reliable form of 2nd factor authentication, especially given occasional delays in receiving OTP's or geo-tagging accuracy issues, both requiring increased dependency on Telecom Network operators. Instead, with many of these same smartphones now supporting biometrics / facial recognition, adding the "what you are" is a more reliable form of authentication that could lead to a "one-click, one-blink" user experience. Additionally, they see increased user confidence in adding the "what you are" authenticator mechanisms to their existing authentication mechanism.

Biometric and 'what you are' tokens: The strongest form of authentication arguably is the biometric authentication. It establishes identity along with the authentication and provides the highest level of assurance. With many mobile devices providing biometric finger print based support, it may be reasonably well established that the same person is accessing biometric enabled application and thus adds Multi Factor Cryptographic support in an untrusted environment. However these biometric authentications are available only locally and performed within a trusted execution environment of the devices.

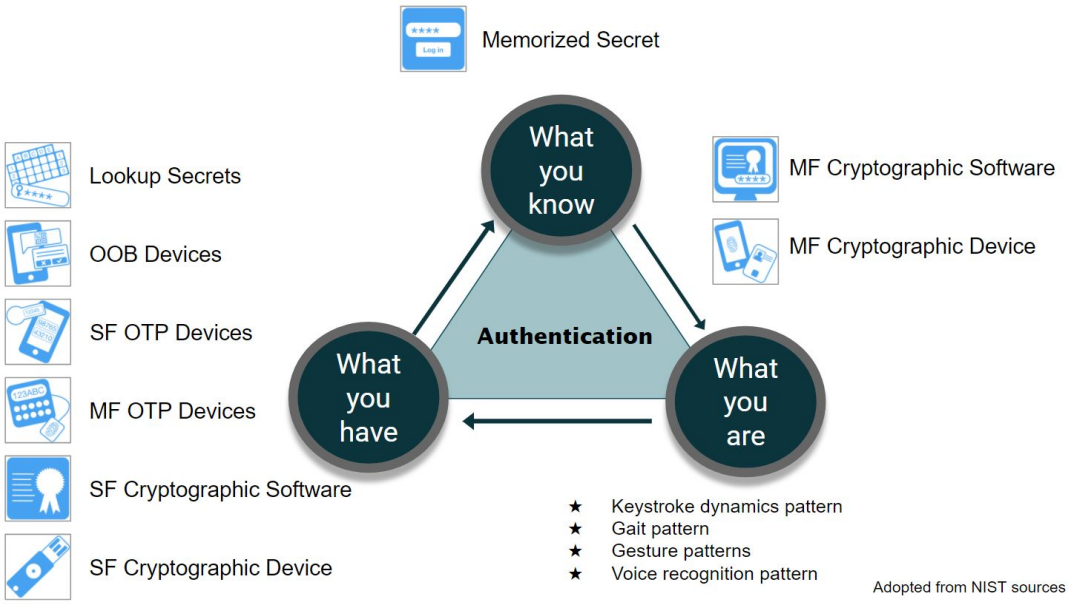
Biometrics are one assured way that ties the digital identifier with real life person, thus has a great potential to enable faster onboarding of customers at the same time reducing costs and diminishing opportunities of frauds.

FIDO technologies and browsers integration

The FIDO UAF strong authentication framework enables online services and websites, whether on the open Internet or within enterprises, to transparently leverage native security features of end-user computing devices for strong user authentication and to reduce the problems associated with creating and remembering many online credentials. The FIDO authentication mechanisms enable biometric authenticators after an initial registration [6].When used as authenticators across multiple devices may ease the authentication process and enable a password-less authentication. In a recent discussions with Sunil Lalvani, Co-Founder and Business Head of Sparsa Secure, we discussed such mechanism where authentication happens on a separate device for a seamless experience.

Summary of authenticators:

The following diagram shows various different authenticator types that are available and lists some emerging AI based biometric authenticators. A combination of strong biometric authenticators and 'what you have' tokens through initial device binding may provide robust frictionless authentication mechanisms.



AI based authenticators

In a recent discussion with Tamaghana Basu, the CTO of a startup company NeoEyed, I learnt about some new modes of authenticator mechanisms which are driven by AI to identify the user based on their typing pattern, gaits and gestures. Dr. V.N. Sastry at IDRBT has been researching the voice based authentication and payment mechanisms. These represents some new frontiers of authenticator techniques which may be added silently to the authentication workflows to build an adaptive authentication mechanism to reduce frictions.

3. Identity

As we interlace our lives between digital and real world the identity proofing provides a means to establish the link between these two world. The KYC requirements before the pervasive growth and integration of ICT systems were not so complex. Usually, the people would provide one or more references to establish a people require digital identity to gain access to application, resources and services. The identity proofing of customers requires acceptability, validation and verification of identity evidence to support their claim of identity. The regulatory norms for KYC requires a certain assurance level and recent master directive update rules for establishing customers identity through Aadhaar based biometric means [2]. Establishing identity with high assurance introduces certain friction into the process and also could be expensive for the organizations. The goals of identity proofing process should then be:

1. Validate that the identifiers provided by the entity is correct and genuine and associated with the person supplying the identity evidence.
2. Validate that a claimed entity exists in real world
3. Develop means to reduce the friction and reduce cost of the identity proofing process

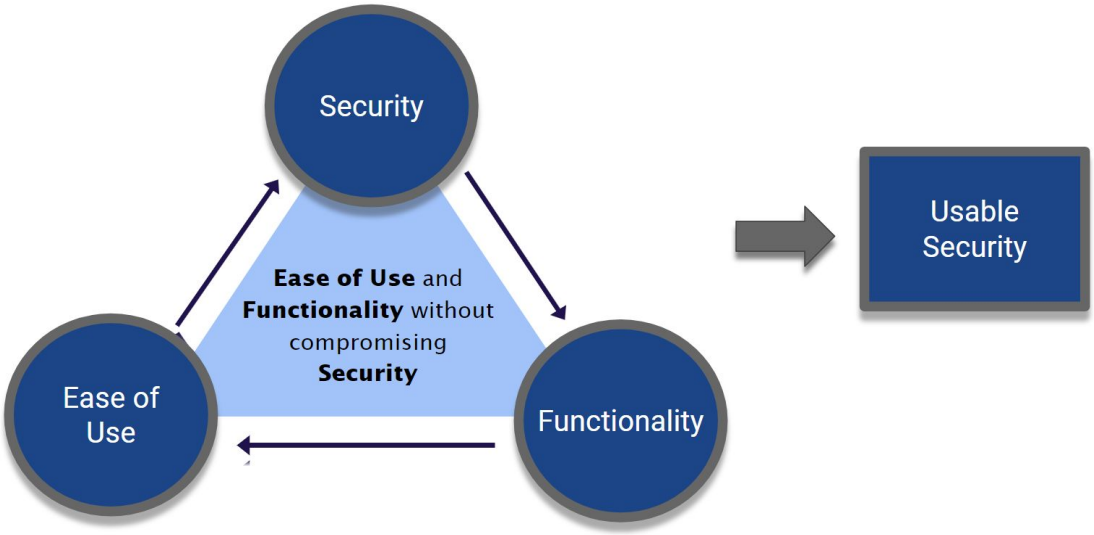
There are multiple categories of digital identifiers, depending upon the verification mechanisms:

Type	Examples	Description
Strong Identifiers	Mobile, Email, Aadhaar	These identifiers can be verified by the means of OTP or biometric authentication and are thus considered strong identifiers.
Weak Identifiers	PAN and other Officially Valid Documents	There is no strong mechanisms to verify that the PAN number that the User has entered actually belongs to the User (even though this can be manually verified).
Functional Identifiers	CRN, Account number, Folio Number	There does not exist a mechanism to verify this. These identifiers must be verified along with the Strong Identifiers, i.e., a combination of CRN and mobile number together is only

		verifiable.

4. Way Ahead

Some of the ideas presented in the article evaluates means and mechanisms of providing strong authentication without compromizing security. In fact, I believe that the technology has sufficiently advanced so that we may be looking at a future where the security is invisible. In the interim, we can strive to strike a right balance between security, ease of use and functionality to get to a usable security.



The reputation based systems, the digital exhaust and footprints, social networks graphs may further be able to help identify individuals and blend digital and physical identities.

5. Terms used/coined in the article

Authenticators	Authenticators are mechanisms used for authenticating a user to a system. These authenticators are classified between, what you know, what you have and what you are.
Adaptive Authentication	The Adaptive Authentication is a mechanism employed in a multi factor authentication systems, where based on certain characteristics such as location, device etc, the authentication mechanism is adjusted to reduce friction in authenticating users.
Cognitive Burden	The Cognitive Burden is a term used to describe the recollection complexity, requirements to create complex password and to

	remember different passwords, authentication mechanisms and the security requirements across different systems.
Device coupled attestation	The proximity of a device such as a mobile phone in proximity of a laptop for example enable the laptop to obtain a confidence measure of the user authentication to a system. This attestation may be used in combination of another authenticator mechanisms to enhance security.
Digital Exhaust	Our activities on the Internet generates digital data and we leave a trail of our activities as we interacts with systems and websites. This is termed as digital exhaust in the paper (I originally heard this term from my industry colleague Subhash Subramanian, ICICI Bank).
Invisible Security	Invisible security as used in this document refers to mechanisms where the security is able to transparently identify and authorize the user to systems that they are authorized for. It may be acheived through a combination of identification mechanisms such as device binding, biometric authentication and single sign on.
Usable Security	Security could introduce friction and when friction comes in the way of us getting things done, people will likely try to circumvent the security. Usable security as defined in this article is the security that minimizes and introduces acceptable level of friction and enable the users to get their work done efficiently.
Zero Friction Security	This this the utopian dream where the security is robust enough and does not require any user explicit interaction to authenticate and authorize the user. This may be acheived using proximity sensors, location awareness, multi-device binding, device coupled attestation, OS level attestation of biometric validation and mechanisms to establish the biometric mapping to the digital world across applications and platforms.
Zero Trust Security	Google introduced this term for their Beyond Corp solution. Unlike the traditional perimeter security model, BeyondCorp dispels the notion of network segmentation as the primary mechanism for protecting sensitive resources. Instead, all applications are deployed to the public Internet, accessible through a user and device-centric authentication and authorization workflow.

6. Reference

[1] "NIST SP 800-63 Digital Identity Guidelines." *SP 800-63 Digital Identity Guidelines*, pages.nist.gov/800-63-3. https://pages.nist.gov/800-63-3/

[2] "Master Direction Know Your Customer", RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16

https://rbidocs.rbi.org.in/rdocs/notification/PDFs/18MDKYCD8E68EB13629A4A82BE8E06E606C57E57.PDF

[3] "The Design of Everyday Things." Wikipedia. June 08, 2018. https://en.wikipedia.org/wiki/The_Design_of_Everyday_Things

[4] Katz, Jessica. "Can We Hack Your Password?" M.A. Polce. September 21, 2017. https://mapolce.com/blog/can-hack-password/.

[5] "Run Zero Trust Security Like Google." BeyondCorp. https://www.beyondcorp.com/.

[6] "FIDO UAF Architectural Overview." FIDO Alliance. https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-uaf-overview-v1.1-id-20170202.html.

Stay Connected

Reserve Bank Information Technology Pvt. Ltd
https://rebit.org.in

LinkedIn
https://www.linkedin.com/company/reserve-bank-information-technology-pvt-ltd

Twitter
https://twitter.com/reservebankit

Email
communications@rebit.org.in

Technology Landscape Briefs

Technology is now embedded deep into the business success. It has the potential to disrupt existing business models even in mature industries. Information technology, which was once a cost center, has now become a strategic business imperative. ReBIT's "Technology Landscape Briefs" are series of papers that touches upon specific technologies or use of technologies as they pertain to financial domain with a focus on "security".

Disclaimer

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. ReBIT disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any act or omissions made based on such information. ReBIT does not provide legal, regulatory, audit or tax advice. Readers are responsible for obtaining such advice from their own legal counsel and other licensed professionals.
No part of this publication may be reproduced, adapted, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the author.

About ReBIT

Reserve Bank Information Technology Private Limited (ReBIT), has been set up by the Reserve Bank of India to serve its IT and cybersecurity needs and to improve the cyber resilience of the Indian banking industry.

Subscribe to ReBIT's Cyber Pulse Monthly Newsletter

https://rebit.org.in/newsletter