UPGRADING AUTHENTICATION MODELS: MFA, PASSWORDLESS AND MORE

Chrysalis Panel Discussion

TECHVISION
CHRYSALIS

Your Presenters

- Pam Dingle, Director of Identity Standards, Microsoft
- Husnain Bajwa, Head of Product Strategy, Beyond Identity
- Doug Simmons, Principal Consulting Analyst, TechVision Research, author of TechVision's series of PAM Reports

What is This Session About?

- We have anticipated the demise of password-centric authentication for decades.
- Due to device and network ubiquity, reliability, Bring Your Own Device (BYOD) initiatives coupled with the accelerating levels of fraud associated with password-based authentication, the time has arrived to deploy MFA or other means of dynamically authenticating given the risk profile within your enterprise.
- MFA is becoming the standard, and password-less authentication, biometrics and other advances in authentication are being brought to market in support of the digital enterprise.
- This session will include a TechVision “level set” and perspectives from selected vendors as to how the user authentication landscape will and should change.

Thesis

- Alternative user authentication methods are gaining traction as a best practice for enterprise security programs.
- It is based on the premise that traditional, single factor authentication schemes (like IDs and passwords) are relatively easy to break and as threats escalate, simply not good enough.
- It is a good time to consider making upgraded authentication schemes a cornerstone of your enterprise IAM infrastructure given improved vendor offerings and the inherent weaknesses of phishing-vulnerable password-based authentication.

Requiring multiple authentication factors for high risk or high value transactions is the emerging security best practice

TECHVISION CHRYSALIS®

Typical Authentication Business Requirements

- ***Business Facilitation*** and the need to improve interoperability and efficiency through interconnected systems to support employees, affiliates, business partners and customers.
- ***Enhancing User Experience*** by simplifying the process of authentication and authorization and letting the end user *not* have to remember another password or provide anything more than basic PII.
- ***Cost Containment*** planning to reduce the cost of management of multiple disparate authentication and authorization systems and processes.
- ***Security Effectiveness and IT Risk Management*** improving the level of assurance that maps to an identity for appropriate authentication and authorization as well as reducing liability by not maintaining unnecessary PII.
- ***Support Administrative and End-user Efficiency and Effectiveness*** By consolidating the authentication/authorization infrastructure and better defining and reducing the number of access points.

Emerging Authentication Models

- Multi-Factor Authentication (MFA) is a subset of the authentication market and is often evoked based on adaptive authentication or step-up authentication based on security policy and/or contextual data regarding the person requesting access
- Typically, one category of 'factors' is something that you know, such as a user ID and password or PIN
- A second factor that is added to this is often something that you have, such as a smart phone, smart card, token fob or other such unique device that when paired with the first factor (something that you know), increases the veracity of authentication
- A third factor can be something that you are
    - Biometrics typically fill this bill with digital representations of your face (facial recognition), fingerprint, retina scan or voice print
- Fourth is something that you have done
    - This can include where you have logged into from before (IP network address), recent transactions, time of day, last password reset, and flags for multiple failed login attempts

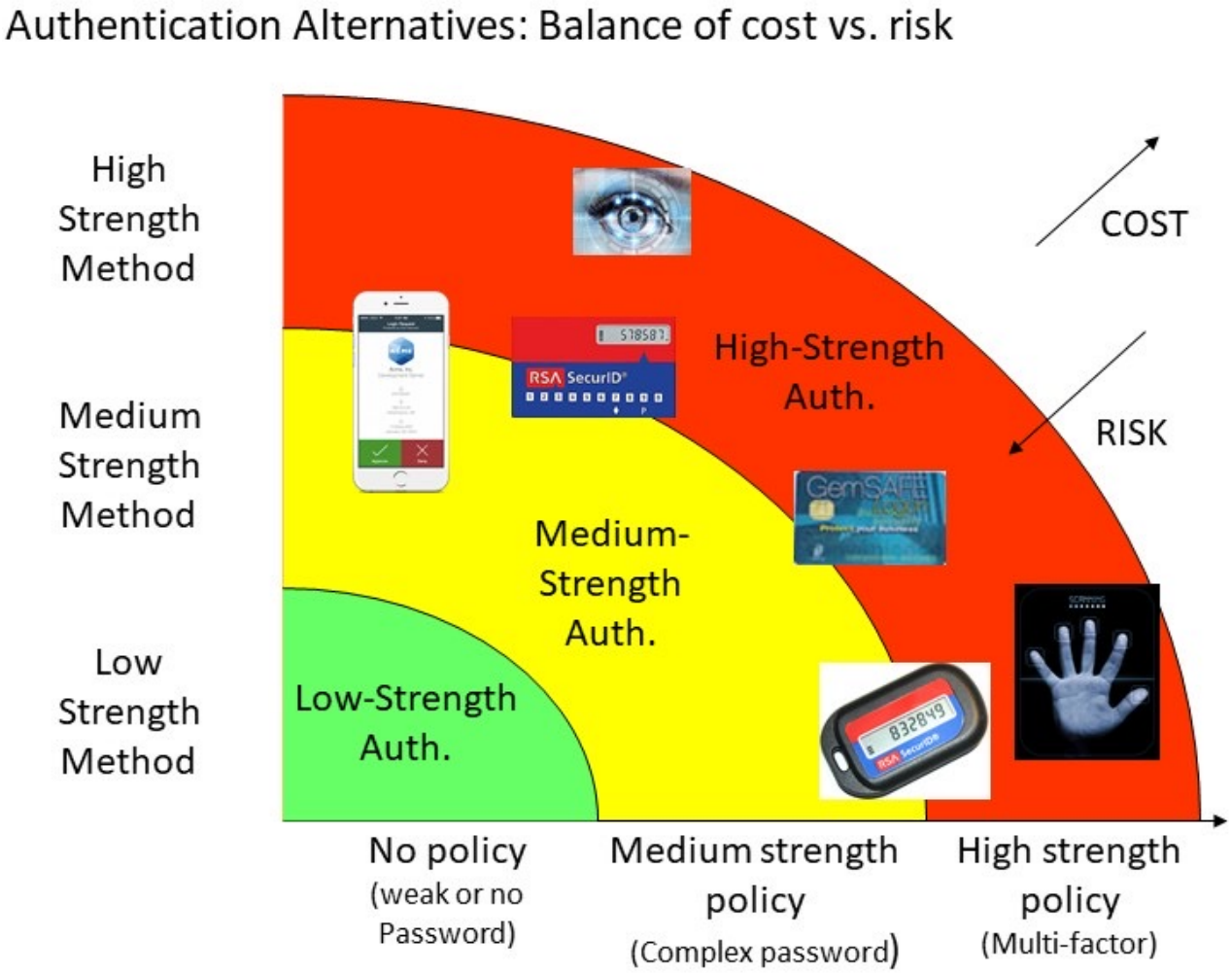
Emerging Authentication Models

- Passwordless Authentication is based on the relatively nascent Zero Knowledge Proof model that eliminates the password or PIN from the picture
- Passwordless authentication relies on a cryptographic key pair – a private and a public key
  - The public key is provided during registration to the authenticating service (remote server, application or website) while the private key is kept on a user's device or in-cloud (e.g., Passkey) and can only be accessed when a biometric signature, hardware token (e.g., Yubikey) or other passwordless factor is introduced.
- In most common implementations, users are asked to enter their public identifier (username, mobile phone number, email address or any other registered ID) and then complete the authentication process by providing a secure proof of identity in the form of an accepted authentication factor. These factors classically fall into two categories:
  1. Something the user **has**, such as a mobile phone, one-time password (OTP) token, smart card or a hardware token such as a FIDO-compliant key fob.
  2. Something the user **is**, such as fingerprints, iris scans, face or voice recognition and other biometric identifiers.

Emerging Authentication Models

- Many emerging passwordless authentication designs also accept a combination of other meta data and contextual factors such as geo-location, network address, behavioral patterns and gestures and so on.
- All are considered passwordless as long as no memorized password or PIN is involved.
- The **FIDO** ("Fast IDentity Online") **Alliance** is an open industry association launched in February 2013 whose mission is to develop and promote authentication standards that help reduce the reliance on passwords.
- FIDO2 (April 2018) provides an extended set of functionality to cover additional use-cases, with the main driver being passwordless login flows.

Enterprise Authentication Decision Points



TECHVISION CHRYSALIS®

Panel Discussion

- How does your solution address the approach to stronger authentication?
- What are the typical obstacles you may be seeing when your customers or prospects want to improve their user authentication capabilities?
- What are one or two of the most significant areas your Product Team is attempting to address in the authentication market?

Questions?

TECHVISION

CHRYSALIS