FIGI Security Clinic

Account Takeover
Why MFA is not Enough

Abbie Barbir, PhD, CISSP
Senior Security Advisor

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

Account takeover

- What is account takeover?
- A fraudster gest access to a legitimate user account
  - All account types vulnerable
- How does account takeover happen?
  - Hacker uses stolen credentials to access a genuine account
  - Hacker may change the account details
  - Hacker users the account to perform financial transactions
  - Hacker may sell account information on black market

How fraudsters get a hold of credentials

1. Phishing with fake websites
   - Criminals set up a website to look exactly like it belongs to a legitimate company
   - Criminals email potential victims to try to get them to click on the link pointing to the site. It is possible to trick users to the fake site to give over their login details.
2. Malware, Trojans, spyware
   - For example a malicious link can lead a user to download key loggers that track what they are typing into login and password fields
3. Social engineering
   - These attacks use psychological tools to manipulate users into giving up confidential data
   - Criminals may call customer support and convince someone to give them access to a user's account (in particular if they know the victim personal info, like SSN)
4. Hijacking a mobile device

Source: http://pages.siftscience.com/

Why fraudsters are flocking to account data

1. Older accounts better trust
   - New accounts are more likely to be flagged for fraud or given more scrutiny
2. Richer data
   - Stolen identities or accounts are a richer form of data than credit card numbers—they can even be used to create new accounts.
3. Longer shelf life
   - Login credentials can typically be used for longer than credit card numbers
4. Businesses playing catchup
   4. Many sites do not invest in proper technology

Source: http://pages.siftscience.com/

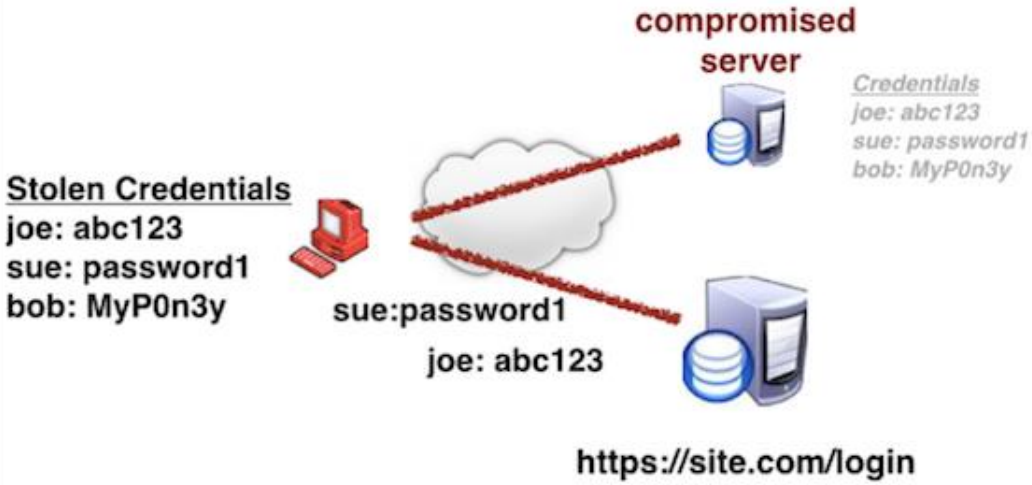
Problems with passwords

- Data breaches / Password Reuse
- Credential stuffing
  - Automated web injection of breached username/password piars in ordere to gain access to user accounts
  - A subset of brute force attack category and a common technique for account takeover

Source: https://www.owasp.org

Anatomy of an Attack

- **Anatomy of Attack**
  1. Attacker acquires spilled usernames and passwords from a site breach or password dump site
  2. Attacker uses an account checker to test the stolen credentials against many websites (for instance, social media sites or online marketplaces).
  3. Successful logins allow attacker to take over the account matching the stolen credentials.
  4. Attacker drains stolen accounts of stored value, credit card numbers, and PII
  5. Attacker may also use account information going forward to send spam or create further transactions



Takeover Attack

How to detect account takeover attack

- Multiple accounts suddenly changing details to the same thing
- New account details, new device and new delivery address
  - The customer has updated a customer detail (telephone, email, name).
  - The customer has had a login from a new device within a 24hour period of that change.
  - After both 1 and 2, the customer has placed an order with a new delivery location.
- Accounts with multiple IP address countries
- Lots of customer detail changes happening at once
- Ratio of known/unknown device models
- Multiple accounts linked to the same device

How to limit the impact of an attack

- Set rate limits on login
  - Rate limits logins: device, username and IP address
- Cross reference login data with existing data
  - Take into account specific login data for device, browser, IP address. Time of day and location
- Check for breached credentials
  - check if a new user has signed up with known breached credentials or if an existing user details have been breached
- Verify a user's identity when they make a change
  - Send a challenge to authenticate to determine real users. Enable two-factor authentication
- Send users notifications of account changes
  - Inform users of their data changes

Source Ravelin.com

How to detect Account takeover

- Behavioral clues
- Signs may be are contained in subtle behavioral patterns across user activity
  1. Login attempts from different devices and locations
  2. Switching to older browsers and operating systems
  3. Buying more than usual, buying higher priced items
  4. Changing device and account settings
  5. Changing shipping addresses
  6. Changing passwords
  7. Multiple failed login attempts
  8. Unusual log out attempts
  9. Suspicious device configurations, like proxy or VPN setups

Source: http://pages.siftscience.com/

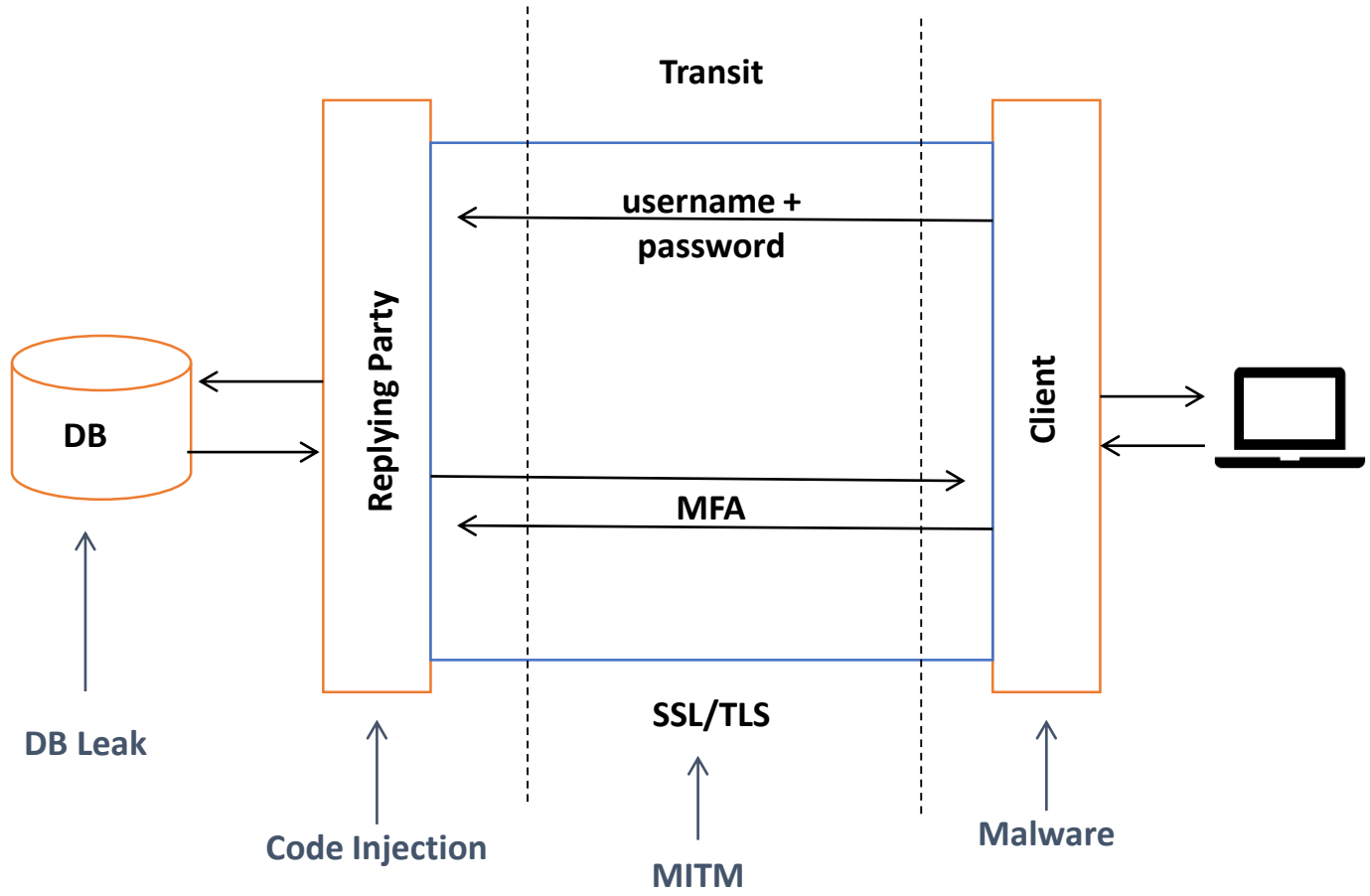
Dynamically adjusting login flows

- By using a risk engine it is possible to dynamically modify users login experience based on risk score
  - For example, if a user's score is low, then you can remove all friction so they can easily sign in and keep engaging on your platform without being bothered with captchas or codes.
  - If the user score is high, you have the option of adding authentication steps to ensure that the user is really who they say they are
  - Can detect user browsing patterns including browser fingure printing
  - Record use typical access address such as network and IP data
  - Map user location history and device information
  - Multifactor authentication can be used to improve risk score. For example:
    - Email or text the user a one-time passcode to enter after login to confirm their identity
    - Email or text an account link that the user can click to approve the new login from a new device
    - Email or text the user a notification of a login from a new device so that they can be aware in case it's not them
    - Limit a user's account actions (e.g., no updating password, no placing orders) until the user logs in again from a trusted device or location
    - Have user fill out a Captcha or image identification

Source: http://pages.siftscience.com/

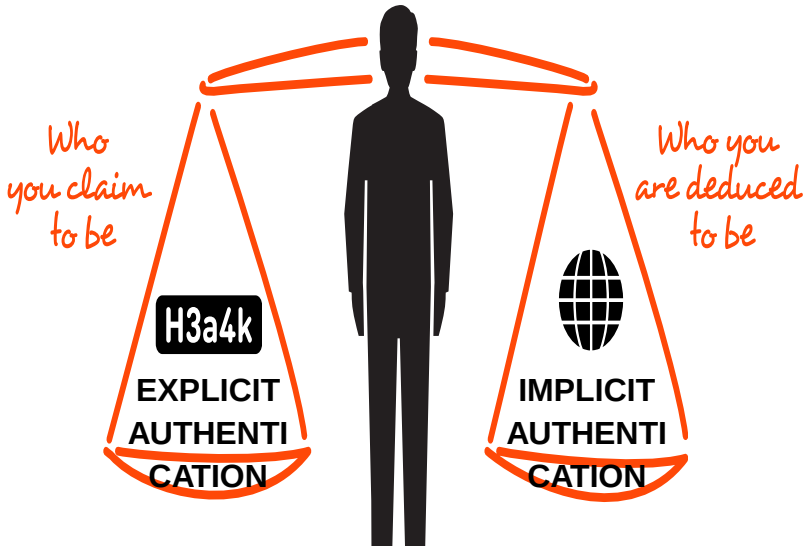
MFA issues

- Passwords
  - Based on Shared Secret
  - Account Take Over risks
  - KBA is easy to overcome
    - Data Breaches
- MFA
  - One of factor from each auth categories
    - Something you Are
    - Something you have,
    - Something you Know
  - Still Phishable
- Device Binding
  - Browser Fingerprinting (BFP)

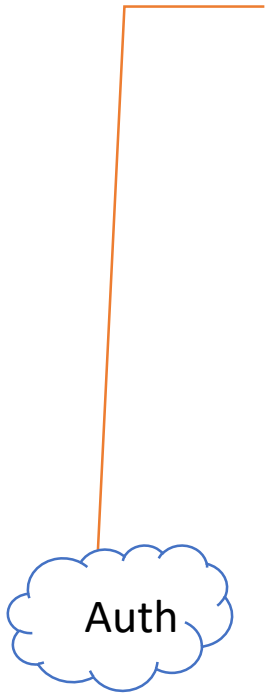


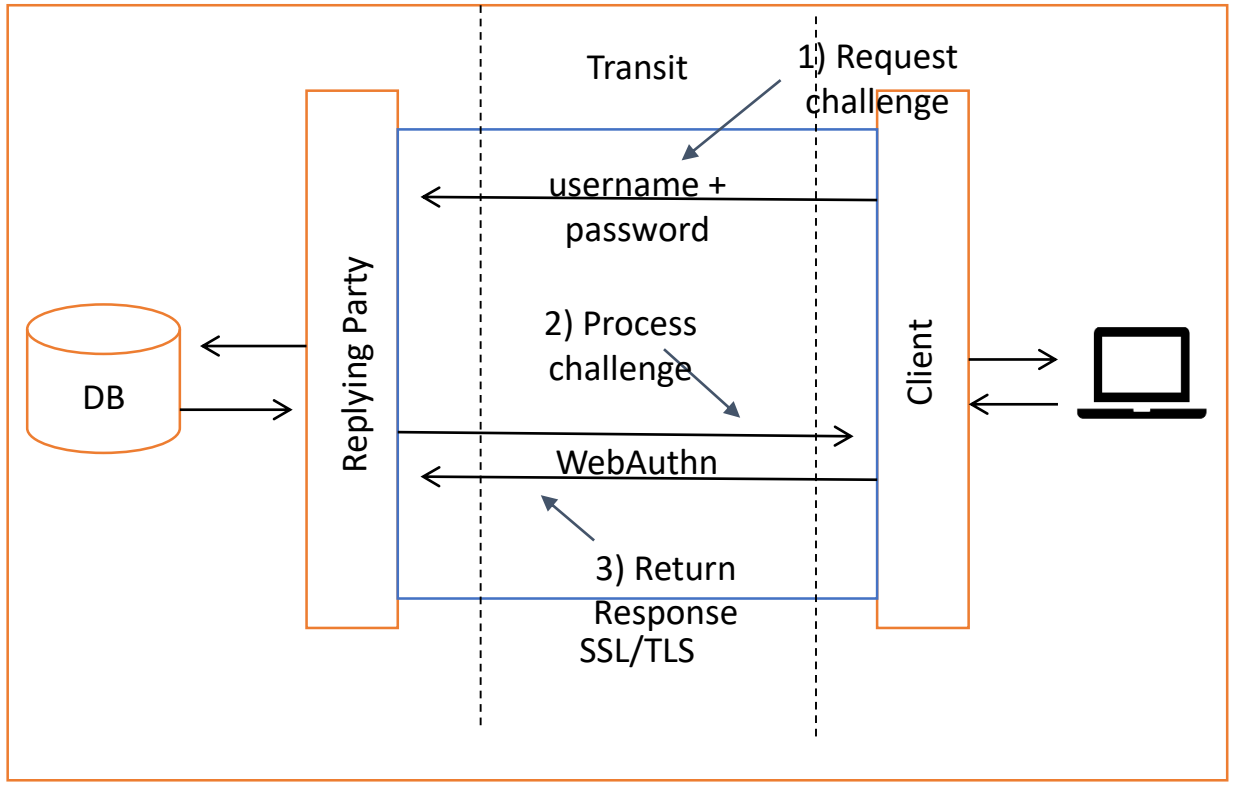
Source: Reece Guida

Modern Authentication - FIDO



- MUST eliminate symmetric shared secrets
- Address poor user experiences and friction
- FIDO is a building block





Create an Account Recovery Plan

- Create an account recovery process
  - If you alert a customer that a change has been made on their account and they confirm it wasn't them, you need to have a process in place to keep their account safe.
  - Draw up the possibilities of how you can recover the account for your genuine customer
  - Place a temporary freeze on the account to prevent the fraudster from making purchases
  - If the fraudster has changed their password, force a password reset with a new, temporary and unique password
- Make sure you have consistent messaging

Source Ravelin.com

FIGI Security Clinic

Cognitive Continuous Authentication

Jorge Coelho

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

Risk-Based Authentication

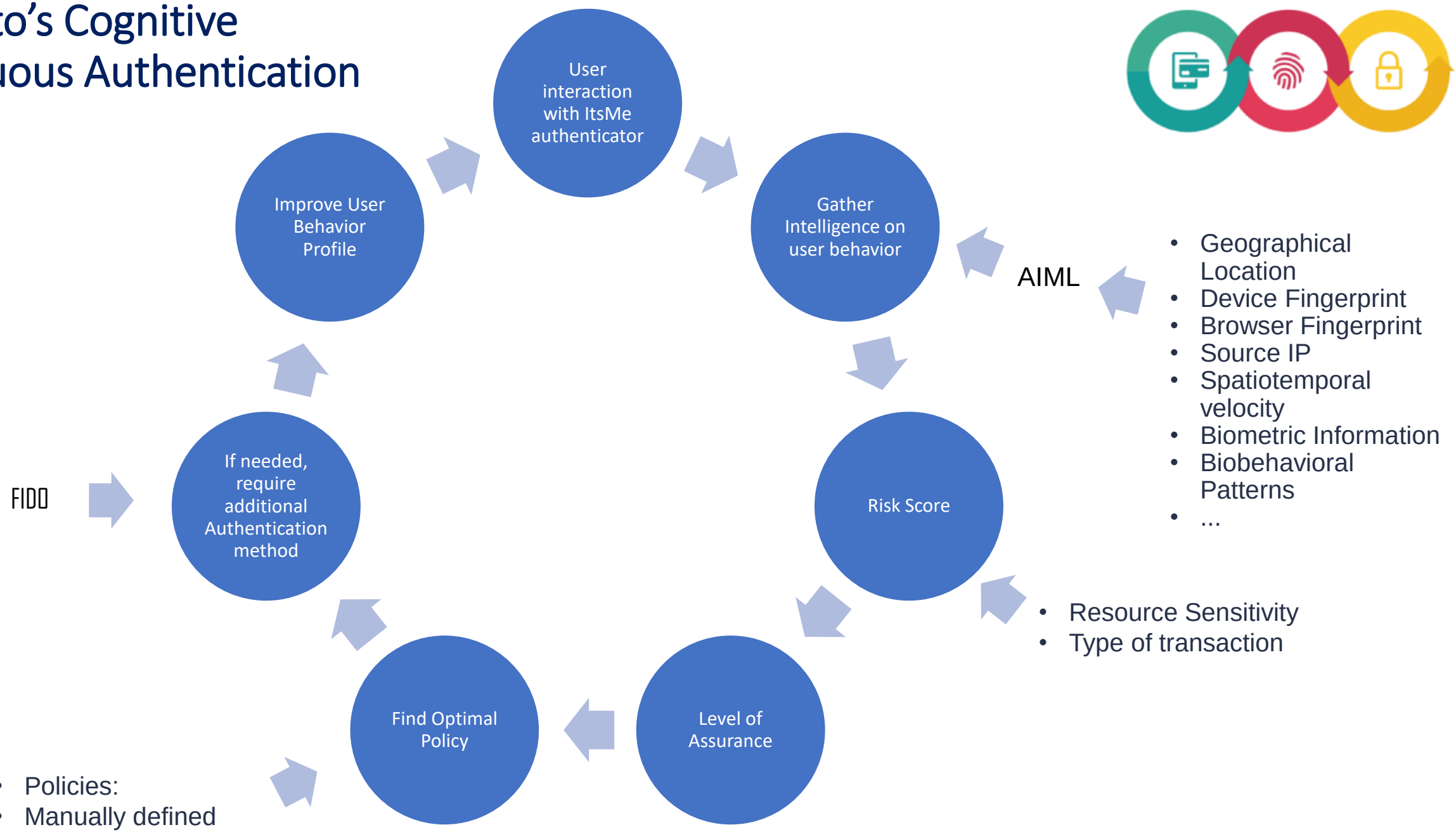
- FIDO provides password-less, secure authentication
  - It doesn't solve some identity theft issues
- Each authentication attempt should be evaluated based on risk
  - Examples of Risk factors detection:
    - Location
      - Collect the geographical location of the authentication attempt
      - Detect anomalies
    - Device/Browser Fingerprinting (DBFP)
      - Collect the characteristics of the device and browser that are performing the authentication attempt
      - Ex. Browser type, browser version, OS, user-agent, screen resolution
      - Detect anomalies
    - Others (Source IP, Biobehavioral patterns, ...)
  - According to the calculated risk, additional multi-factor authentication steps may or may not be required

Acceptto's Cognitive Continuous Authentication

- Creating a password-less authentication system involves issues that are not solved by FIDO
  - Credential Management (accounts with multiple authenticators, account deletion and recovery, ...)
  - Identity proofing
  - Post-Authorization continuous authentication

- FIDO + Risk Based Authentication + AIML = Acceptto's Cognitive Continuous Authentication
  - Provides a Multi-Factor Authentication system on top of FIDO
  - Access is granted via policies based on sensitivity of transactions and resources
  - AIML engine creates user behavior profiles that ensure additional authentication methods are required if needed
  - Strong user identity proofing (Email, SMS, Device Fingerprint, Corporation Filter, ...)

Acceptto's Cognitive Continuous Authentication



Questions?