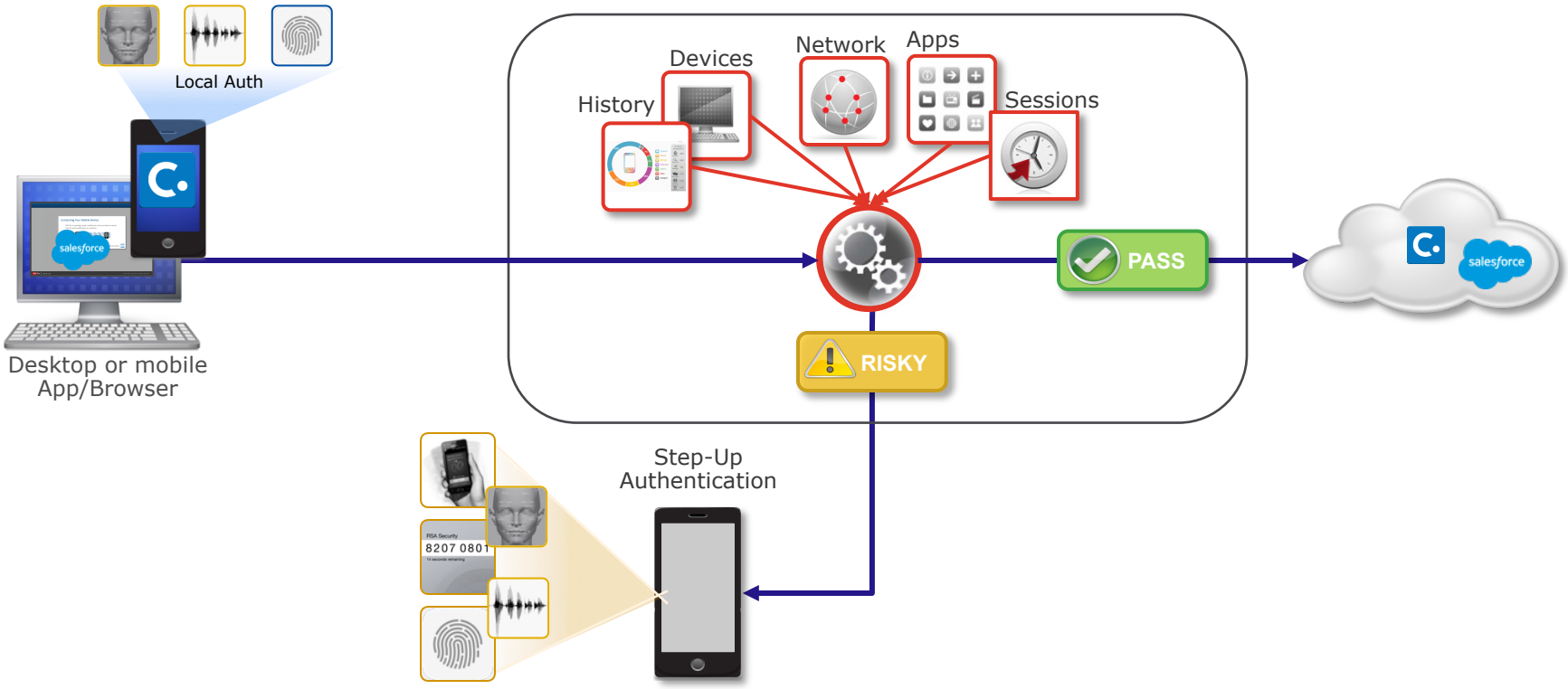
RISK ←→ Auth

How Big Data Enables building Risk Profiles

Kayvan Alikhani

RSA, Senior Director of Technology

RISK BASED AUTHENTICATION



Why not solely rely on biometrics?

Challenges with Biometric Auth:

- "Biometric data" in the wrong hands **can** cause harm
- Biometrics Auth methods are **not** fool proof
- Malicious access **can** occur using "Biometric data"
  (not different from any other authentication data)

Challenges: Biometrics Doesn't "always" work

- Fails for the **right** user for the **wrong** reasons:
  - *Live-ness detection can make biometric inconvenient to use*
- Environment dependencies:
  - *Too much noise*
  - *Too little light*
  - *Too much light*
  - *Shared environment, need to lower voice*
- For remote auth methods:
  - *Connection too slow (auth takes too long/times out)*
  - Security concerns about access to server-side bio data

Challenges: Device dependency

- Biometric Method “A” Only Works on Model “x” of device vendor “y”
- Biometric Data is not “well protected” on device “x”
  - *Device “x” is not equipped with SE/TEE, can’t protect biometric data @ rest*
- Biometric Method “A” stores actual templates on the device/ server, making hacked access a huge vulnerability
  if you thought Password leaks were bad…

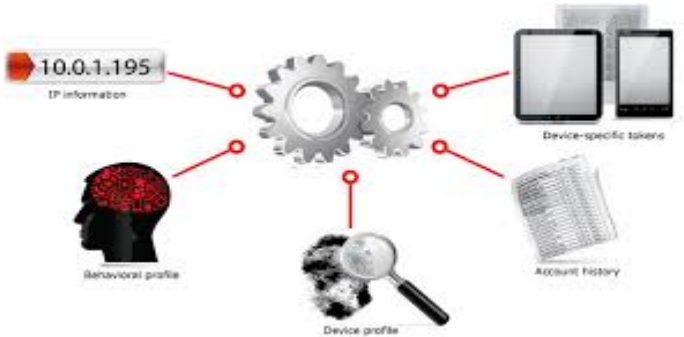
So there's risk involved…let's use multi-factor

- **Adapt**:
  - Use multi-factor Authentication **only** when needed
  - Context sensitive: *Use App/Action sensitivity & **risk** to determine auth level*
  - Minimize friction: Transparently authenticate lower-risk actions
  - Adapt to users, regardless of whether they are customers/employees
- **Avoid**:
  - Maintaining endless **static** rules:
    Not scalable to create rules like: *If user at location x then do y…*
  - Sending user credentials (of any kind) over the wire
- **Decide**:
  - Make decisions based on risk assessment:
    If device appears to be compromised, avoid biometric/Out-of-band SMS

Detect Anomalies

- **What is Anomaly detection?**

Finding "*an observation that deviates so much from other observations as to arouse suspicion that it was generated by a different mechanism*"

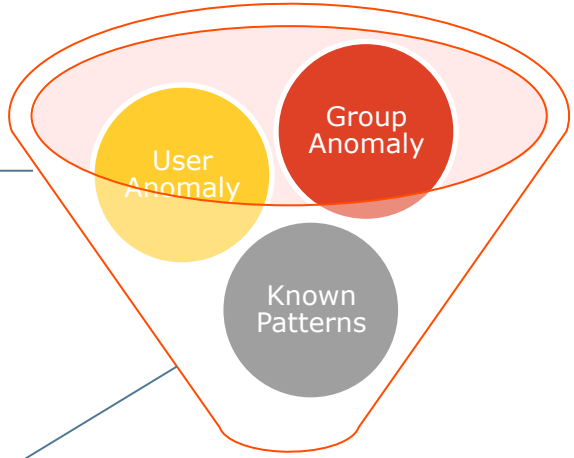


Looking for:

Outliers or Rare events

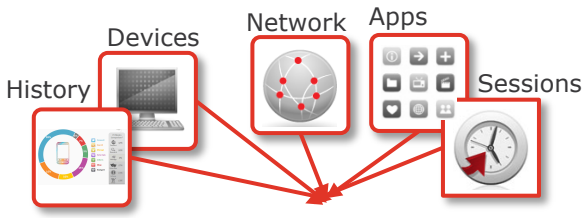
"Huh, that looks odd/funny…"

Anomaly Detection -> Risk assessment



What info is being collected?

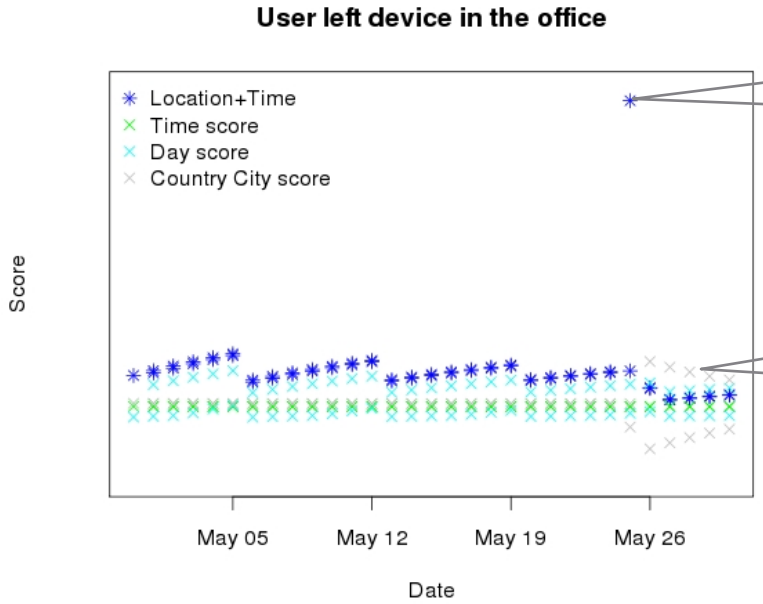
- **Network info:** Wi-Fi/mobile registration
- **Device info:** Capabilities, Hardware ID, MAC address
- **User info:** Identifiers, Roles, Usage & Auth History



- **Session Info:** HTTP headers & end points resources
- **Location info**: Longitude/Latitude, IP-Geo
- **Environment**: Bluetooth, SSID, date & time and TZ

Example

- Scenario:
  - User left a device at the office, overnight
  - Someone tried to use it!!



Correlating location + time + history can discover the **anomaly**

Time, location or history separately would report **normal** behavior

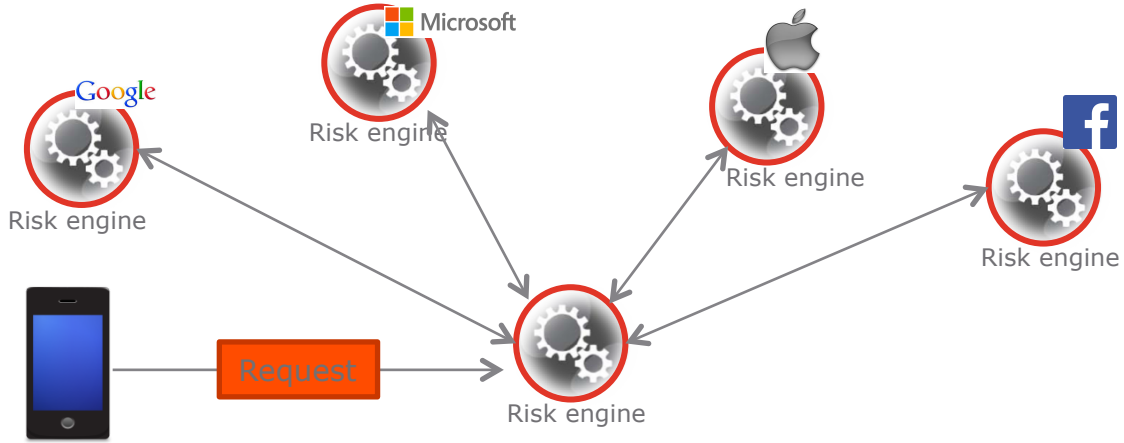
Challenges with Risk-based auth

- Needs big-data!
  *Only as good as the **info collected** & models built*
  - Limited input -> Poor Risk assessment
  - Services **optimize** user interaction -> Less is **known** about the user behavior

- Limited Scope/visibility:
  - User activity within one “scope” is not available to other scopes

Utopian view: The TRAP ecosystem!

- Trusted "Risk Assessment" Partners (TRAP!) :->
  - Can I "trust" this request coming into my service?
  - What do you know about this user/device? What can you share with me?
  - Can we agree on score normalization?
  - Can we use the OS to help us 'trust' the device/user?
  - Can we make this all invisible to the user? Continuous behavioral auth?
- "Maybe" as part of Open ID/Connect combined with FIDO?



EMC²