RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: **EZCL-R09**

Multifactored Auth Bypass: How to Armor Up

Dan Houser

Senior InfoSecurity Manager
The American Chemical Society

NEW Interactive Format!

Topic Intro & Launch

15 Minute Q&A

Table Discussions

Round Robin Readout

Why do we have MFA?

Super Spy Technology Cool

…But does it work?

Problems with Enterprise MFA

- Presumption of path
- Bad Factors
- Compromised Platforms
- Two terrible factors = secure?
- Padlock on a tent
- To a hammer, every problem is a nail

- Falls short of independence
- House of cards built on sand
- People issue with technology solution
- Single factor establish/reset
- 1 Trick Pony
- Many more

Presumption of path

- Front Door

Back Door

Presumption of path

- Bad guys don't read your use cases or follow rules
- Armoring happy path, not all paths
- Need to do a walkabout
- What are all the ways in?

Broken Factors

- PASSWORDS – Known horrible, why we have MFA
- BIOMETRICS – Lots of failure modes
- SMS - Compromised & decertified by NIST as factor
- PHONE CALL – Readily spoofed, relies on Caller ID
- EMAIL – Notoriously easy to bypass / phishing top risk vector
- SECRET Q&A – Horrible, decertified by NIST as a factor

Broken Platforms

- MOBILE: MDM lockdown keeping pace with change
- BROWSER: Common compromise & Man-in-the-Browser
- HUMAN FACTOR: Phishing/Smishing, 419, social engineering
- EMAIL: Largely broken model full of holes
- HELPDESK: How may I help you *(break into a real account)*?

Challenges with MFA:
Cascade Failure in Web of Trust

- Compromise of one account often enables compromise of others:
- Personal email -> phone carrier reset -> new SIM -> OTP token reset

  email -> banking account bank credential reset -> $$$

- Reset of a credential ALWAYS relies on other credentials

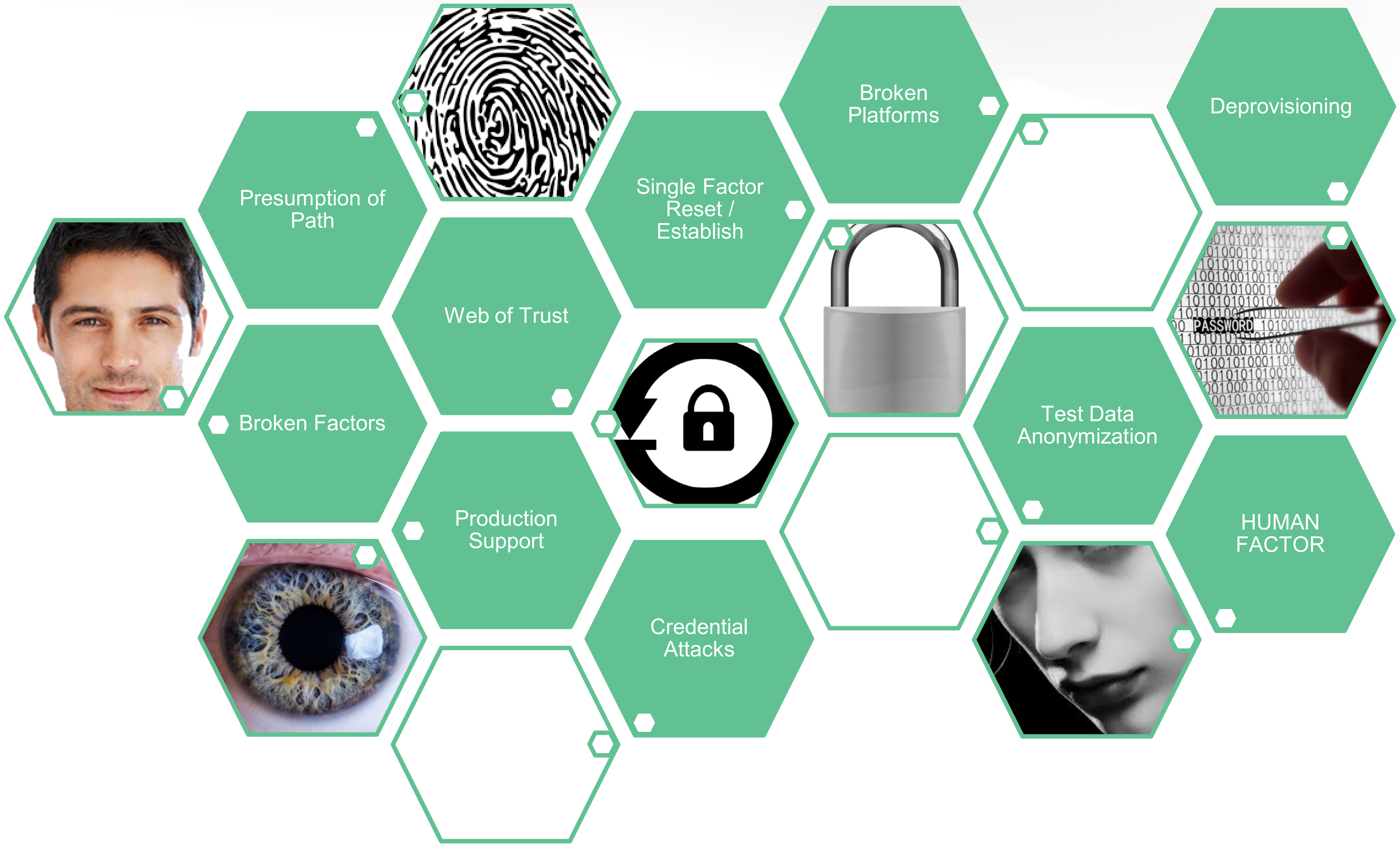
  Most are in-band, and most are single-factor

PASSWORD RESET IS THE WEAKEST LINK OF ALL!

Padlock on a tent

- Varied identity verification methods
- Helpdesk scripts, hints & tricks
- Production support modes
- Test data anonymization & deidentification proofing, all factors?
- Deprovisioning
- Administrative privileges
- Periodic evaluation/assessment
- Weak credential proofing
- Velocity / abuse monitoring, all authenticating paths

Q&A



Presumption of Path

Broken Factors

Web of Trust

Production Support

Single Factor Reset / Establish

Credential Attacks

Broken Platforms

Test Data Anonymization

Deprovisioning

HUMAN FACTOR

How do we Armor Up?

Quick house rules:

- No monologue, try to be terse
- No recording
- Please share & keep on point
- No vendor pitches
- Chatham House Rule: Anyone can be quoted anonymously

Suggested topics

Dealing with broken factors / platforms

Password establish / reset, soft underbelly

How to get MFA lifecycle to zero single-factor auth?

Analytics on all paths in

Elimination of passwords

Can you find all credentials? All AuthN paths? All Federation points?

Credential firewalling & zones of use?

Feedback loop…

Surprises?

Lightbulb moments?

Common Challenges?

RSA®Conference2020

That’s a wrap folks!

Contact info:

Dan.houser@gmail.com

@SecWonk

Will work for bourbon. Consultation for free if you hand me a drink. ☺

APPENDIX

Guiding Principles

NIST 800-63-3, worth a read

- Strong user experience emphasis
- Realistic security expectations, many things need MFA
- Put burden on the verifier, not the user
- Only ask the user to do things if they improve security
- Determine strength via lists, not algorithms

- Free CloudFlare API for password validation:

  https://tinyurl.com/CDIC-Password

Getting Started

- Next week:
  - Identify critical credentials and repositories
  - Create a plan for getting credentials mapped and controlled
- Next 3 months:
  - Inventory all credentials, paths, flows for establish & reset
  - Normalize identity verification standards & scripts
- Next 9 months:
  - Instrument velocity checks on all authentication paths
  - Create backup MFA plan / solution
  - Migrate insecure credentials; consider NIST 800-63-3 as credential standard