RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: SDS-W08

Hacking Advanced Authentication and Armouring Identities

Daniel Houser CISSP-ISSAP CSSLP CISM

Sr. Manager, InfoSec Engineering
CAS – The American Chemical Society
@SecWonk

Why do we have MFA?

Passwords suck

Multi-Factored Authentication

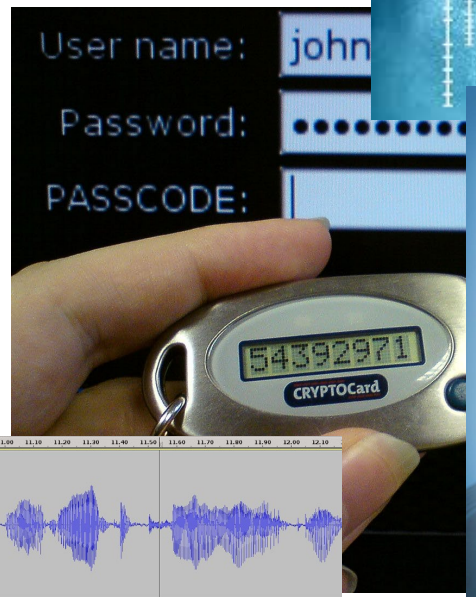
Combines:

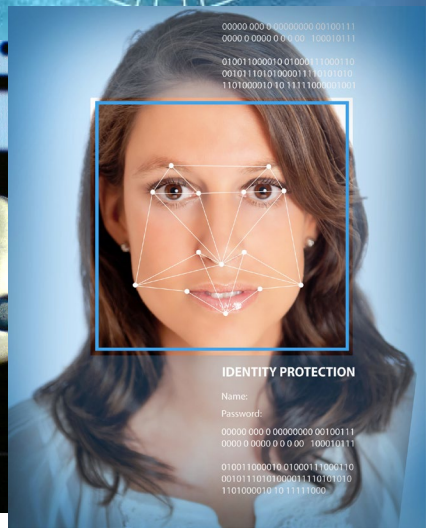
- Something you know — PIN, password, demographics, challenge-response
- Something you have — OTP token, phone, employee access card, key fob, RFID
- Something you are — fingerprint, voice print, photograph, facial recognition

- Fourth factor: Somewhere you are
  - Does transactional activity indicate this logically is the same person?
  - Is Alice currently in Singapore?

Broad adoption by industry

- Facebook, Twitter, WhatsApp, Amazon, etc.
- Mandated by banking regulators
- Mandated by fiat: healthcare, PCI-DSS, governments
- SingPass 2FA mandate 4-July-2016
- **Reasonable standard of due care?**





CAS®
A DIVISION OF THE
AMERICAN CHEMICAL SOCIETY

RSAConference2019
Asia Pacific & Japan

RSAConference2019
Asia Pacific & Japan

But does it work?

But does it work?

First Principles

- Authentication – verification of claimed identity
- Multiple Factors – more than one
- Controls – measures that modify risk
- Based on that measure, yes, for constrained use cases
- For Enterprise MFA? …. Sort-of??
- But is that enough?

Several Problems with Enterprise MFA

- Presumption of path
- Reliance on factors to actually work
- Two terrible factors = secure?
- Padlock on a tent
- 1 Trick Pony
- Falls short of independence
- House of cards built on sand
- People issue with technology solution
- Biometrics, Mobile Auth and the Field of Fail
- Many more…

Presumption of path

MFA is the hardened front door…

Why go in the front 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?

https://www.wizardsbank.com

Wizards Bank

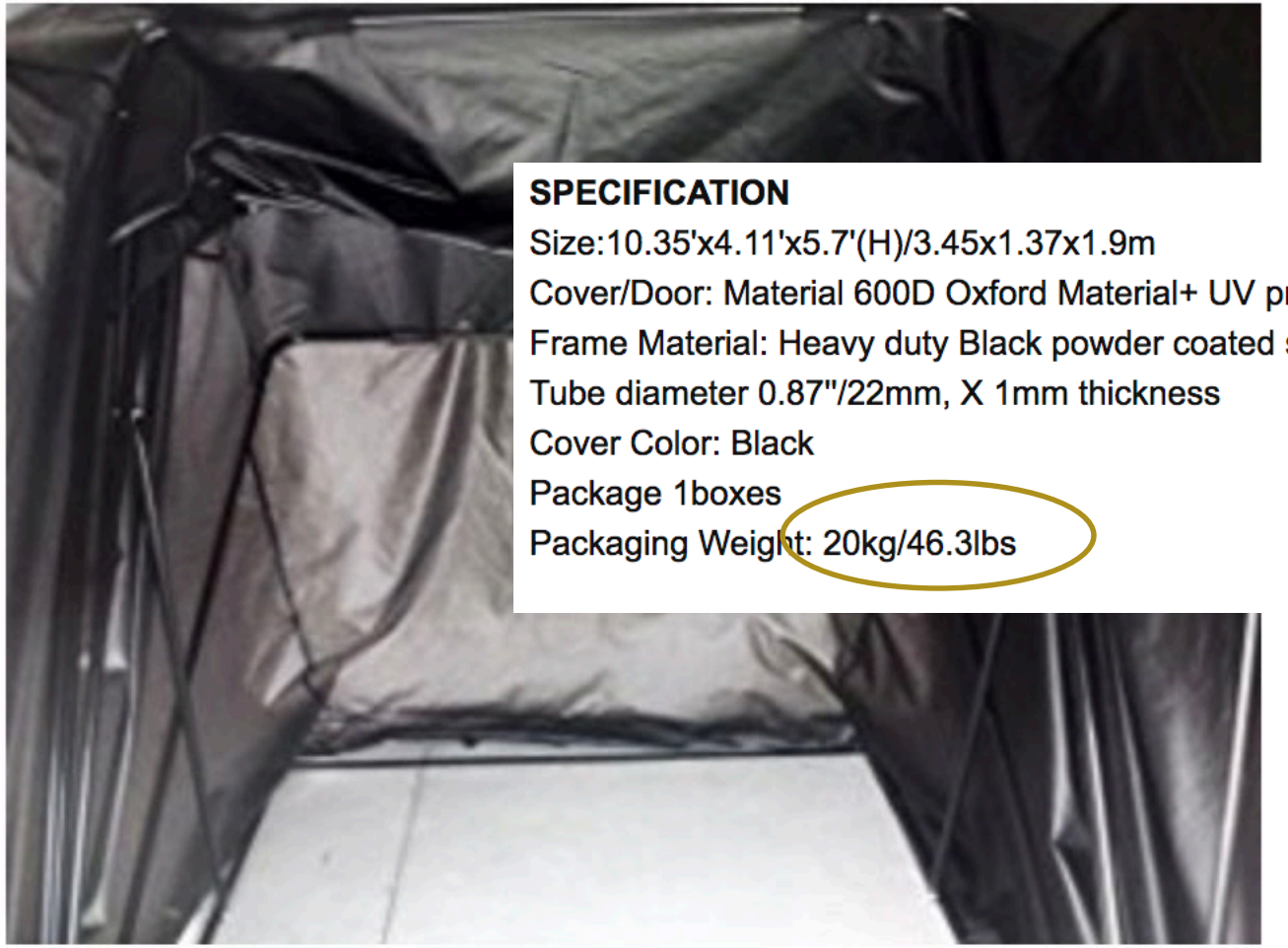
Ministry | Transfers | Galleons to Muggle | Sign In

Flue powder chat with a personal banker now

The lock icon.
PERFECT AUTH. PERFECTLY AWFUL.

- The lock icon is to indicate authentication to the user
- Perfect authentication for engineers
- Horrible for usability

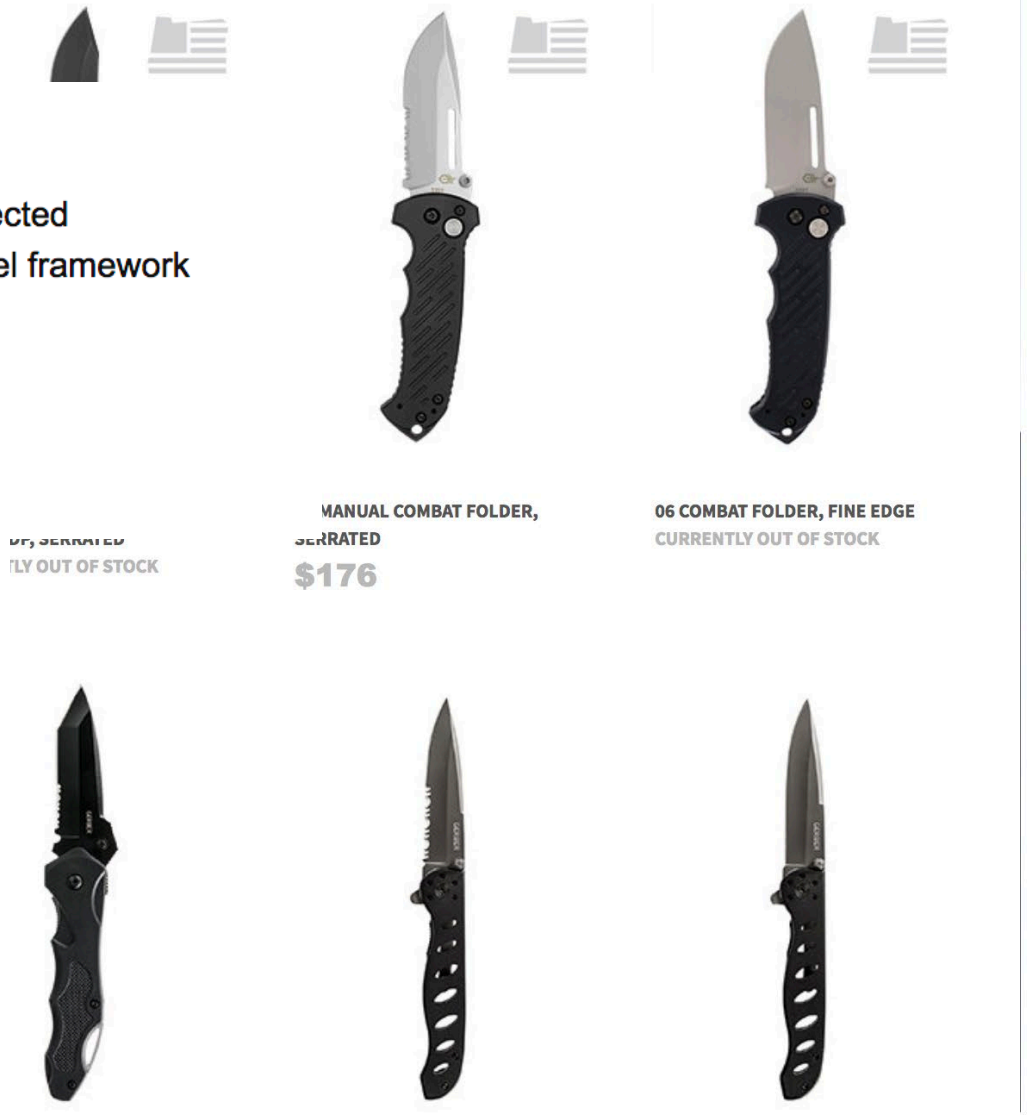
- Engineers are great at building technical solutions, but security and authentication are human processes
- Engineers **believe** they create **technically sufficient** solutions to human problems



SPECIFICATION

Size:10.35'x4.11'x5.7'(H)/3.45x1.37x1.9m
Cover/Door: Material 600D Oxford Material+ UV protected
Frame Material: Heavy duty Black powder coated steel framework
Tube diameter 0.87"/22mm, X 1mm thickness
Cover Color: Black
Package 1boxes
Packaging Weight: 20kg/46.3lbs

Waterproof, Oxford Fabric PU coating on inside entire 1200mm H2O/m, the highest water repellence process on outside and protects from harmful UV light.



MFA: A Field of Fail
Broken authenticators: Broken Factors

SMS is compromised, yet broadly deployed as MFA technology

- SS7 & VOIP attacks, phone forwarding compromises of SMS
- NIST has formally said that SMS isn't an OOB authenticator (7/2016)
- Still broadly used for pre-auth (MFA) and post-auth (Was This You?)

FAIL MODE: Using broken protocols like it didn't matter

MFA: A Field of Fail
Broken authenticators: Broken Factors

Webmail addresses undermine integrity

- Friend at RSA, “So many banks send SecurID tokens via FedEx, then permit credential reset via Hotmail”
- Your customer & employee identity is protected by a Yahoo mail password

FAIL MODES: Pretending free webmail = enterprise email = ISP email

MFA: A Field of Fail
Broken authenticators: Broken Factors

Passwords

- We all know they are TERRIBLE, the reason we have MFA
- However, is password still one of your credentials?
- If you have password + SMS as “2 factors”, you are using two KNOWN BROKEN authentication methods

- Passwords: because humans can’t do X.509
- System passwords: ~~because a computer needs to impersonate a human impersonating a computer?~~
  - Because developers are lazy

Broken Factors: Secret Questions / Answers

- TERRIBLE (killed off by NIST-800-63-3)
- Static question lists lead to easy hacking of answers

  Worst:
  - Favorite type of pet, with drop-down list (dog, cat, fish, bird, reptile, other)
  - What color is the sky?
- My brother can answer most of mine
- Social Media contacts can answer yours… might as well post password?
- Reuse of answers, with no external indicators when Q/A are stolen/breached

Broken Factors: Secret Questions / Answers

Courts haven't ruled yet – Is Q&A personal data covered by breach notification laws??

More reasons Q&A is terrible:

- Inability to manage Q&A atomic lifecycles
- Inability to protect Q&A just like passwords

FAIL MODES: Treating Q&A different than passwords + ignoring OSINT

MFA: A Field of Fail
Broken authenticators: Human Factor

- Automated Phone calls break the human factor
  - Demonstrate phone call attack, Azure MFA call
    - Step 1, gather password of target
    - Step 2, create super-annoying audio clip
    - Step 3: WarVOX Caller Spoofing Wardialing fakes out CallerID
    - Step 4: Launch repeated dialing attack at 3am.

MFA: A Field of Fail
Broken authenticators:

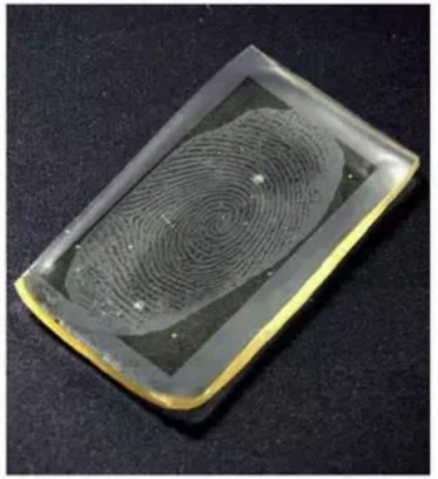
- SMS & Caller ID spoof, easy Smishing

CAS
A DIVISION OF THE AMERICAN CHEMICAL SOCIETY

MFA: A Field of Fail
Broken authenticators: Human Factor

- Theft of phone:
  - Brother Orange, Kim Kardashian, Kit Harrington, etc.
- Mobile carrier account takeover (enroll new SIM/EIN) via social engineering
- Compromised endpoints

Challenges with MFA:
Biometrics is a Field of Fail



Gummy Finger: 50JPY/piece

- Biometrics look super-cool, have TV crime stopper splash
- Rarely deliver across all needed use cases
- Fingerprints
  - Gelatin fingerprints able to bypass many fingerprint scanners in use
  - MSU researchers broke into Samsung Galaxy S6 using conductive paper
  - Bolt cutter attack is pretty unpleasant, but warm oxygenated saline = scanner bypass
- Facial Recognition
  - iPhone X facial recognition fail: mother/son & twins
  - Facial recognition fooled by photographs (Samsung Galaxy Note 8, Win10, etc.)
  - Compromises with statues & 3D printed busts, as life-recognition often fails test
- Typing analytics readily compromised

Challenges with MFA:
Independence of Auth Mechanisms

Mobile Platforms for Commerce, Payments, Social Media & Authentication

- Browser
- eMail
- Shopping app
- OTP token app
- SMS

- Single platform, many low trust & high-trust transactions come together

Challenges with MFA:
Mobile phone as terrible factor

- Man-in-the-middle, public WiFi, compromised GSM, AT&T vulnerabilities
- Broken cryptography (RSA-2048, SSLv3, SHA-1, MD5, RC4) still broadly in use
- DNS exploits
- Phone malware takeover (intercept e-mail, spoof SMS, intercept QR-code)
- Jailbroken phones & unpatched Android
- 35% have no password lock on their phones, 52% of Android users
- Smudge attacks on smartphone touch screens
- All running on compromise engineering principle devices with hidden vulnerabilities and insecure supply chains running buggy software created by low-bid contract by lazy developers with incomplete biased testing to level of minimal sufficiency run by PHBs and with minimal/no consistency in patching

Image source: https://www.usenix.org/legacy/event/woot10/tech/full_papers/Aviv.pdf

Challenges with MFA:
Independence of Auth Mechanisms

- Mobile phone is frequently all in-band, no OOB signaling
  - Different channels, all by same OS & machine

- Attackers have leveraged malware to break down mobile auth wall
- Malware interception of email
- Malware interception of QR code + race & DoS

Challenges with MFA:
Cascade Failure in Web of Trust

- Compromise of one account often enables compromise of others:
- Personal email -> social media -> banking credential reset -> corporate credential reset -> phone carrier reset -> new SIM -> OTP token reset -> cryptocoin wallet unlock…
- The challenge here is that reset of a credential ALWAYS relies on other credentials, and most are in-band
- **Password reset is the weakest link of all**
- FAIL MODES: Single-factor auth as control for multi-factor auth

QED: Single-factor auth for password reset must die.

RSAConference2019
Asia Pacific & Japan

How can we armour up?

Identity Proofing: Armour Up

We must armour the Identity Proofing process

- **No factor used in MFA should be changed without MFA**
- Understand what questions are asked, and how identity is established – **all channels, all methods**
- Establish (and test) bare minimum standards for authentication?
- Establish higher level of authentication for app & system admins
  - Step-up Authentication in your Identity Proofing
- Determine prescribed fall-back steps:
  - Call their manager?
  - Visit the security desk at a facility?
- Defined hints with Zero-tolerance policy for rule bending

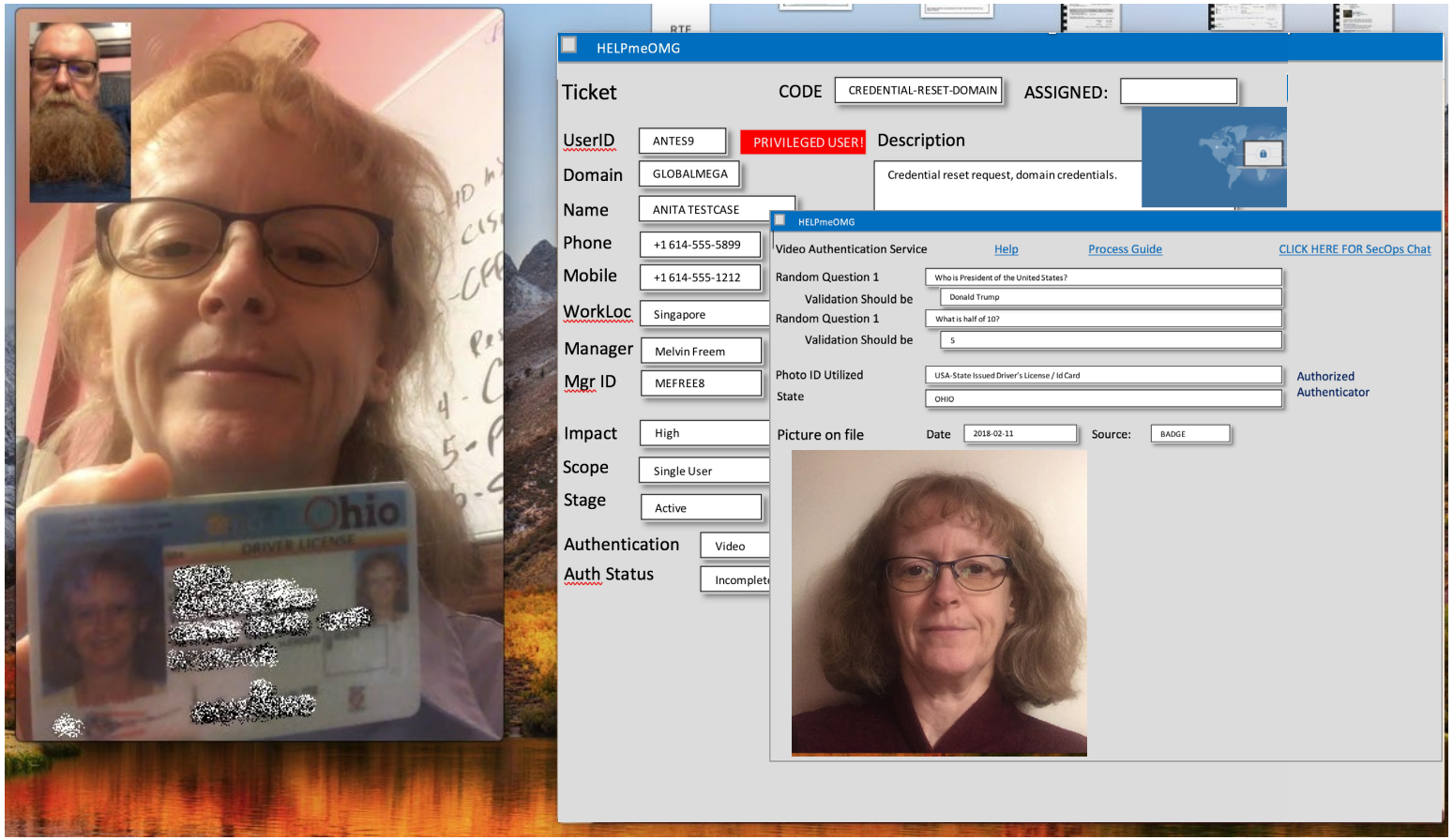
Identity Proofing: Armour Up

Video Credential reset

Compare file photo with live video of associate showing government issue photo ID

Ask random question

- What is 7 x 4?



Identity Proofing: Armour up

Of particular concern is the protection of identity used as factors, or used by authentication interfaces:

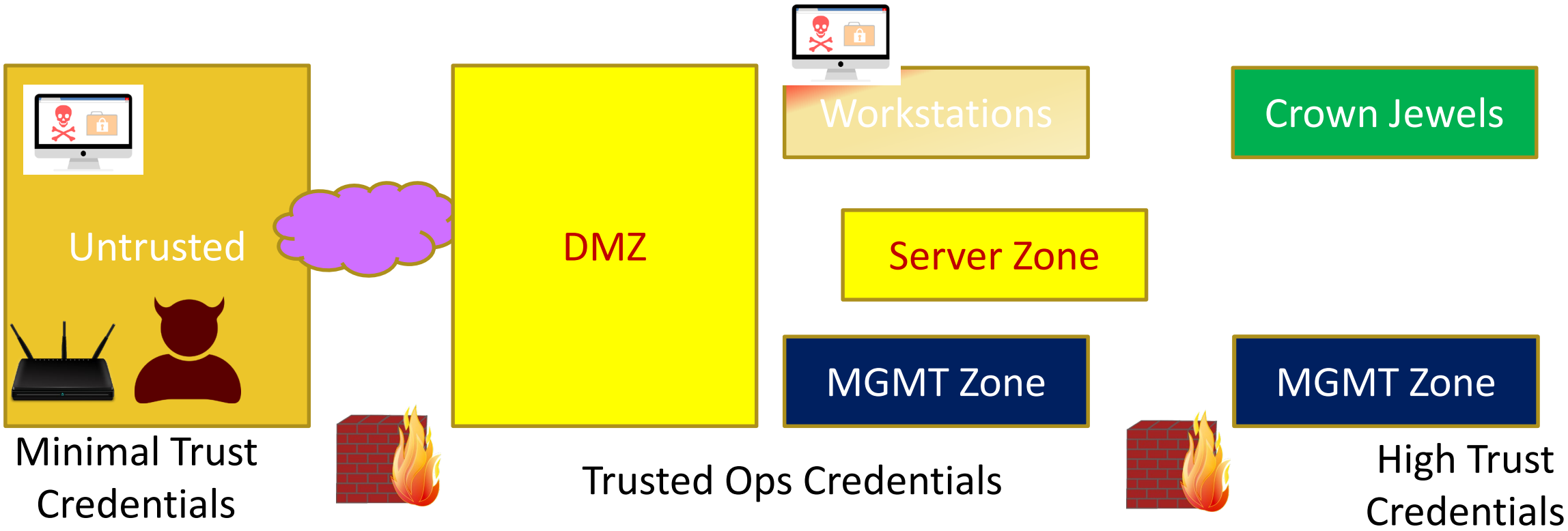
- Mobile & home phone numbers on file
- Home Address
- Location data
- Challenge- Response questions (OMG please kill these now)
- Employee ID
- Home email address
- Voicemail

- Changes to these should trigger more extensive security processing

Credential Firewall

- Privilege escalation on low-trust network (e.g. open desktop zone) should not lead to privilege exploit of crown jewels
- Privileged user accounts should not be typed on untrusted assets
- System accounts / admin accounts for crown jewels should be segregated, ZERO TRUST

Credential Firewall



Necessary Steps to Armour up

- **Knowledge and Inventory of ALL credentials**
  - Trusted: Badge, UserID/Pwd, OTP token, OTP Soft-Token, Voicemail PIN, Parking Sticker, Signature, Identity Q&A, Laptop key, Fingerprint…
  - Federated: Passport, Driver's License, License Plate…
- Policies for Levels of Trust & validation processes
- Standards for Sufficiency of credentials as a factor
- Visibility for In-band vs. Out-of-Band
- Knowledge, Inventory & Governance of ALL credential repositories
- Knowledge, Inventory & Governance of ALL credential reset values

Detection

- Hackers will try 10,000,000 passwords against an account
- Sneaky hackers will try 3 password guesses against all accounts
- Smart hackers will try multiple interfaces and probe the weakest one
- All authentication interfaces need to inform event management
  - Web
  - WiFi
  - Human interaction (e.g. Helpdesk)
  - Desktop
  - Phone/VRU
  - Voicemail
- Detect excessive failure attempts from same IP/location/interface

Your existing MFA is Legacy

- What is good enough today will NOT be good enough forever
- If your MFA solution is 0wned, now what? Do you have a backup?
- What is your MFA Business Continuity Plan?
  - Fail Shut is not a continuity plan
  - Fail Open is not a career plan
- Have two independent MFA solutions in place in case one must be retired
- Ensure you have a robust set of credential factors

Guiding Principles

NIST 800-63-3, worth a read

- Strong user experience emphasis – if not user friendly, they cheat
- 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
- Etc.

"Apply" Slide

- Next week you should:
  - Identify critical credentials and repositories
  - Create a plan for getting credentials mapped and controlled
- Over the next 3 months you should:
  - Inventory all credentials, paths, flows for establish & reset
  - Normalize identity verification standards & scripts
- Within 6 months you should:
  - Instrument velocity checks on all authentication paths
  - Create backup MFA plan / solution
  - Migrate insecure credentials; consider NIST 800-63-3 as credential standard

RSAConference2019
Asia Pacific & Japan

Q&A

Contact info: Dan.houser@gmail.com @SecWonk

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