Password-less Strong Authentication

OWASP, Dallas, TX , May 17th 2016
Be Secure with No Passwords

Girish Chiruvolu, Ph.D., MBA, CISSP, CISM
Information Security and Risk Management

How Would You Choose Your Team?

Every member is a STRONG one to ride rough waters

Familiar?

Anthem healthcare system was breached by attackers software
February 19, 2014

Sony pictures hacked – loss of revenue and disclosure of internal employee information
May 2014

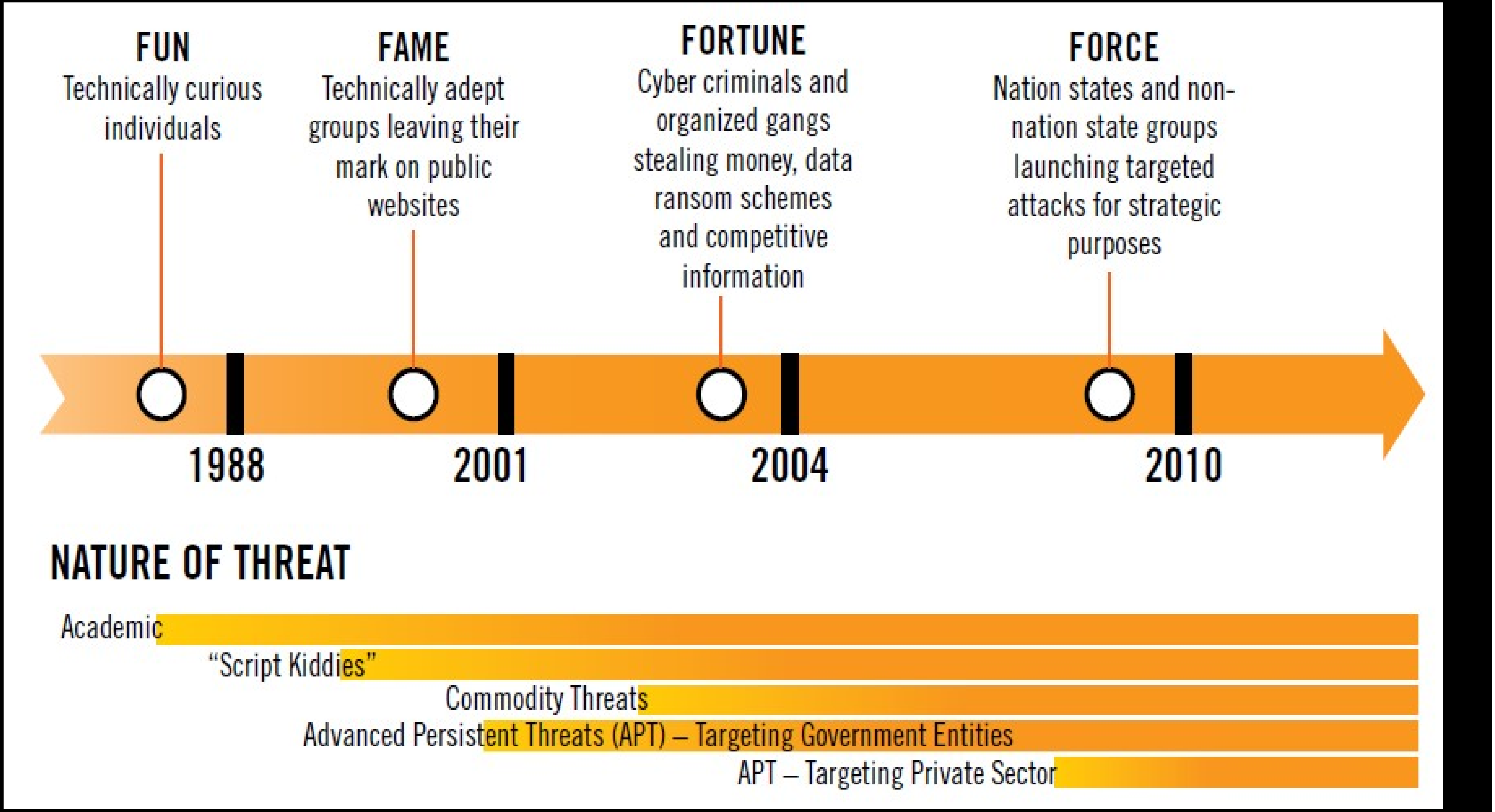
1.5million accounts compromised
June 2014

More than 2 million credit cards compromised
Sept 2014

The entire Ashley-Madison business operations paralyzed *June 2015*

Hackers in got credit and debit card numbers and sensitive information
April 2014

Evolution of Cyber Security Threatscape



FUN
Technically curious individuals

FAME
Technically adept groups leaving their mark on public websites

FORTUNE
Cyber criminals and organized gangs stealing money, data ransom schemes and competitive information

FORCE
Nation states and non-nation state groups launching targeted attacks for strategic purposes

1988

2001

2004

2010

NATURE OF THREAT

Academic

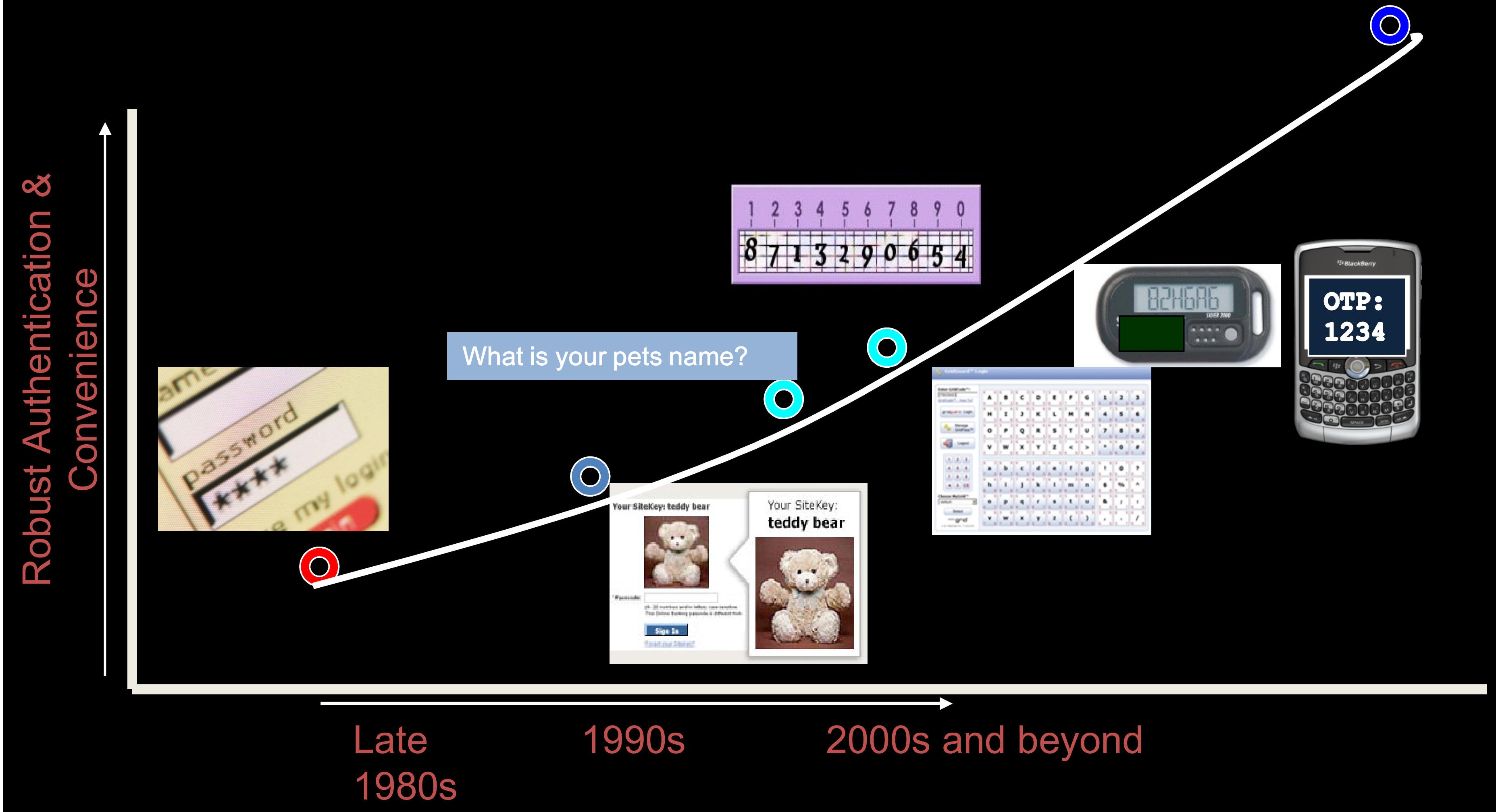
"Script Kiddies"

Commodity Threats

Advanced Persistent Threats (APT) – Targeting Government Entities

APT – Targeting Private Sector

Authentication Jungle



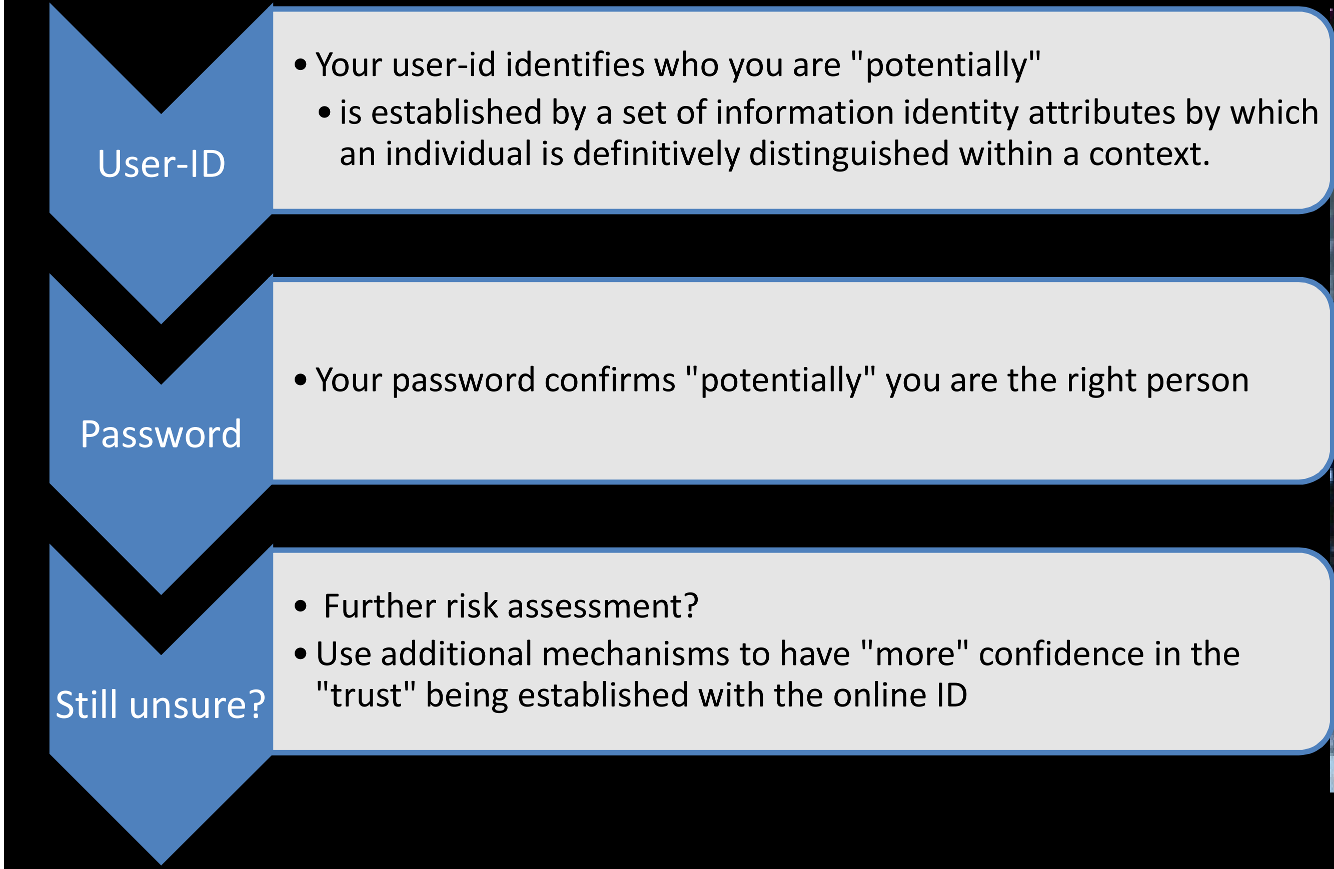
What is your pets name?

Online Identity and Why So Important?

"On the Internet, nobody knows you're a dog."

$5.9 B online fraud in '14

How do You Establish Online Identity?



User-ID

- Your user-id identifies who you are "potentially"
  - is established by a set of information identity attributes by which an individual is definitively distinguished within a context.

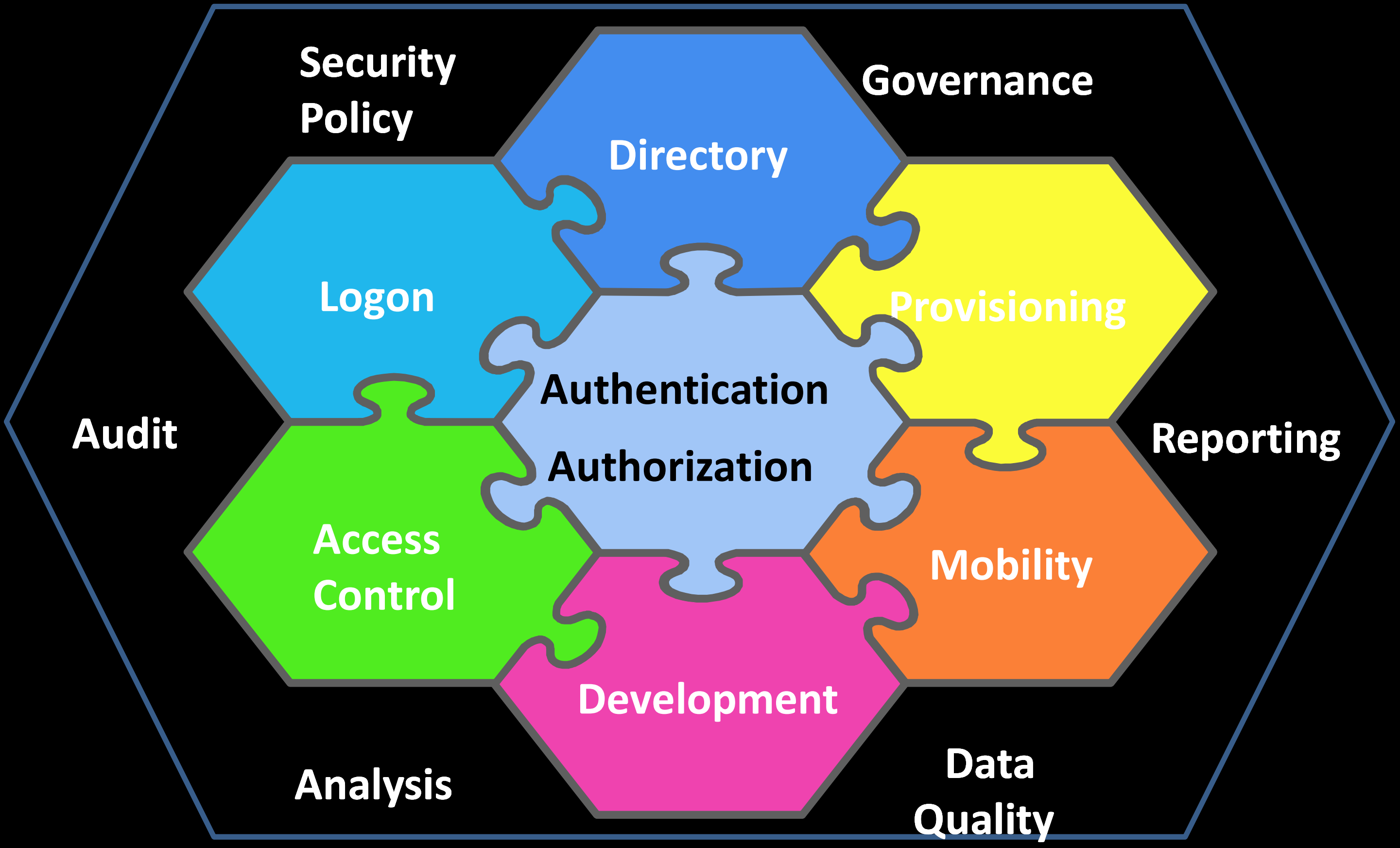
Password

- Your password confirms "potentially" you are the right person

Still unsure?

- Further risk assessment?
- Use additional mechanisms to have "more" confidence in the "trust" being established with the online ID

Information Security and Risk Management



Good Authentication is all about Balancing

Zero client footprint & easy to use

Convenience

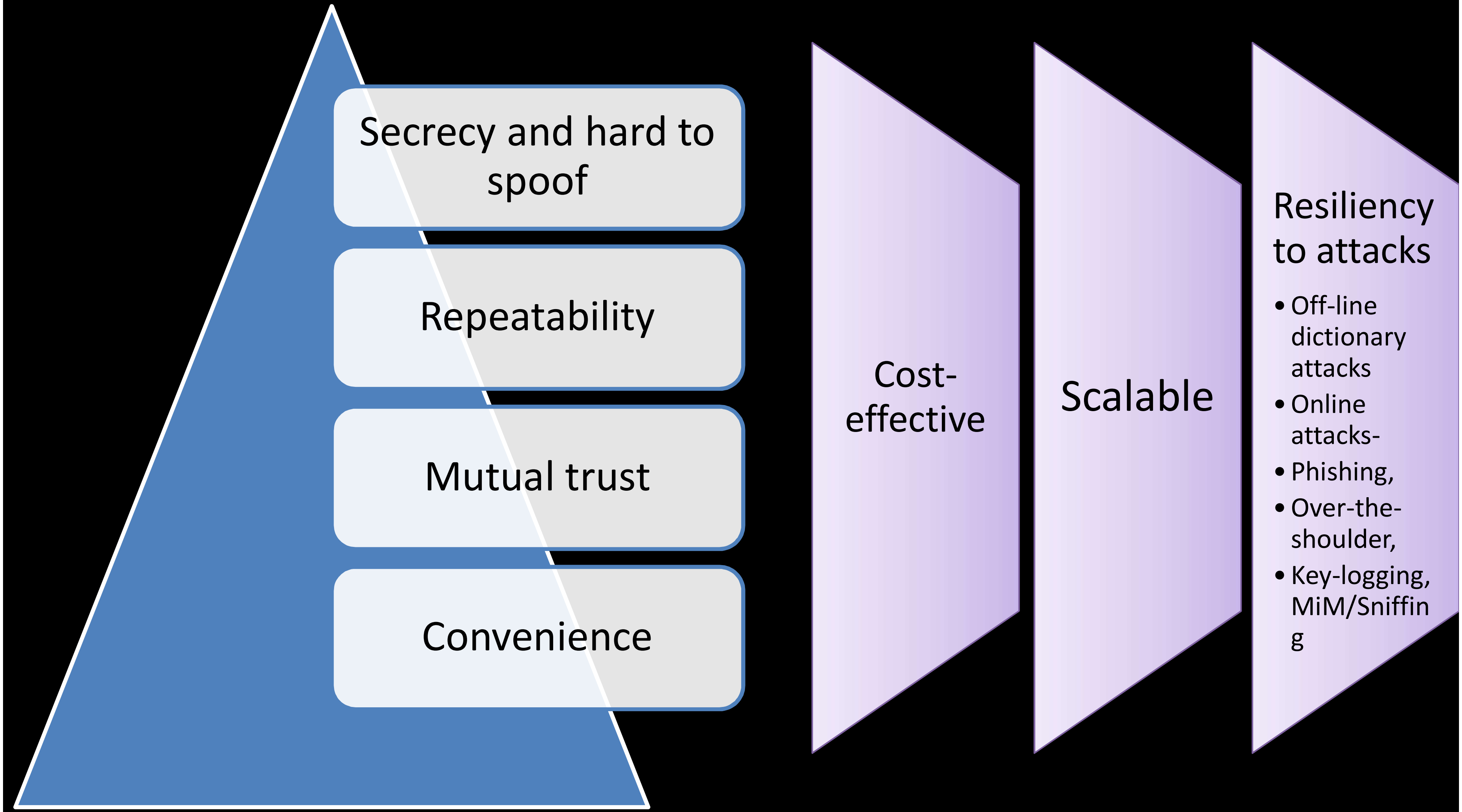
Cost

Security

Low cost of implementation & maintenance

Robust security with device-less disposable password; resilient to Man-in-Middle attacks, etc.

Good Characteristics of Online Authentication



Secrecy and hard to spoof

Repeatability

Mutual trust

Convenience

Cost-effective

Scalable

Resiliency to attacks

- Off-line dictionary attacks
- Online attacks-
- Phishing,
- Over-the-shoulder,
- Key-logging, MiM/Sniffing

Closer Look at Passwords!

English has a maximum entropy of 6 bits per character

Typical pure random password of 6 characters = 36 bits of entropy

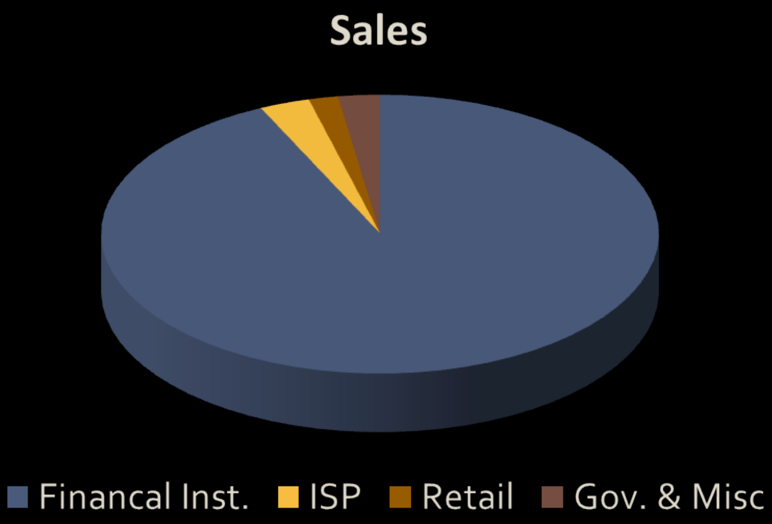
Typical human generated passwords → Much less entropy

My password: letMe1in

- Strong Passwords hard to remember – I%&killer$#144Pwd+
- “Social engineering”
- Finding written password : Post-It Notes
- Guessing password: Spouse/Kid DoBs etc.
- Shoulder surfing
- Keystroke logging
  - Virtual keyboards/mouse
- Screen scraping (with Keystroke logging)
- Brute force password crackers (Rainbow tables –hash tables, salts)
- **Password explosion (SSO and Fed-SSO)**

The SOS Signal on (1st Factor) Passwords

At least $1B Online Fraud Annually



Average = $120/online user*

*Sources: RSA annual report 2014

USA TODAY

Banks seek customers' help to stop online thieves

Updated 1d 16h ago

By Byron Acohido, USA TODAY

By Alejandro Gonzalez, USA TODAY

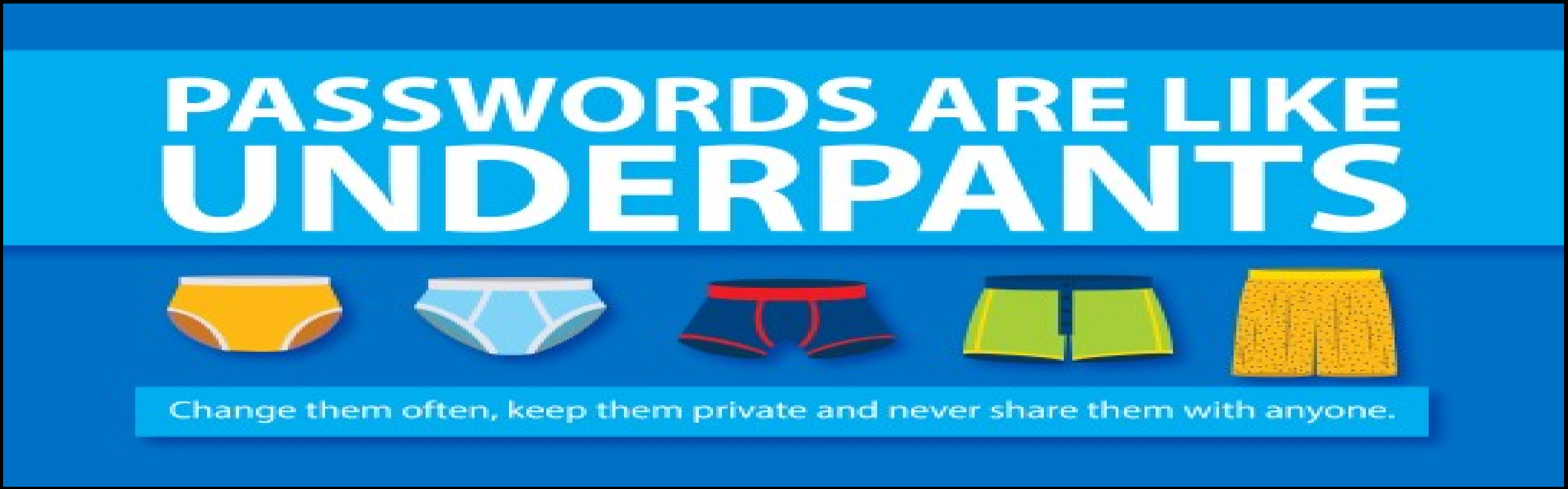
Industry Quotes

- “Passwords are like toothbrushes….

  You don’t lend them out

  and you change them often!”

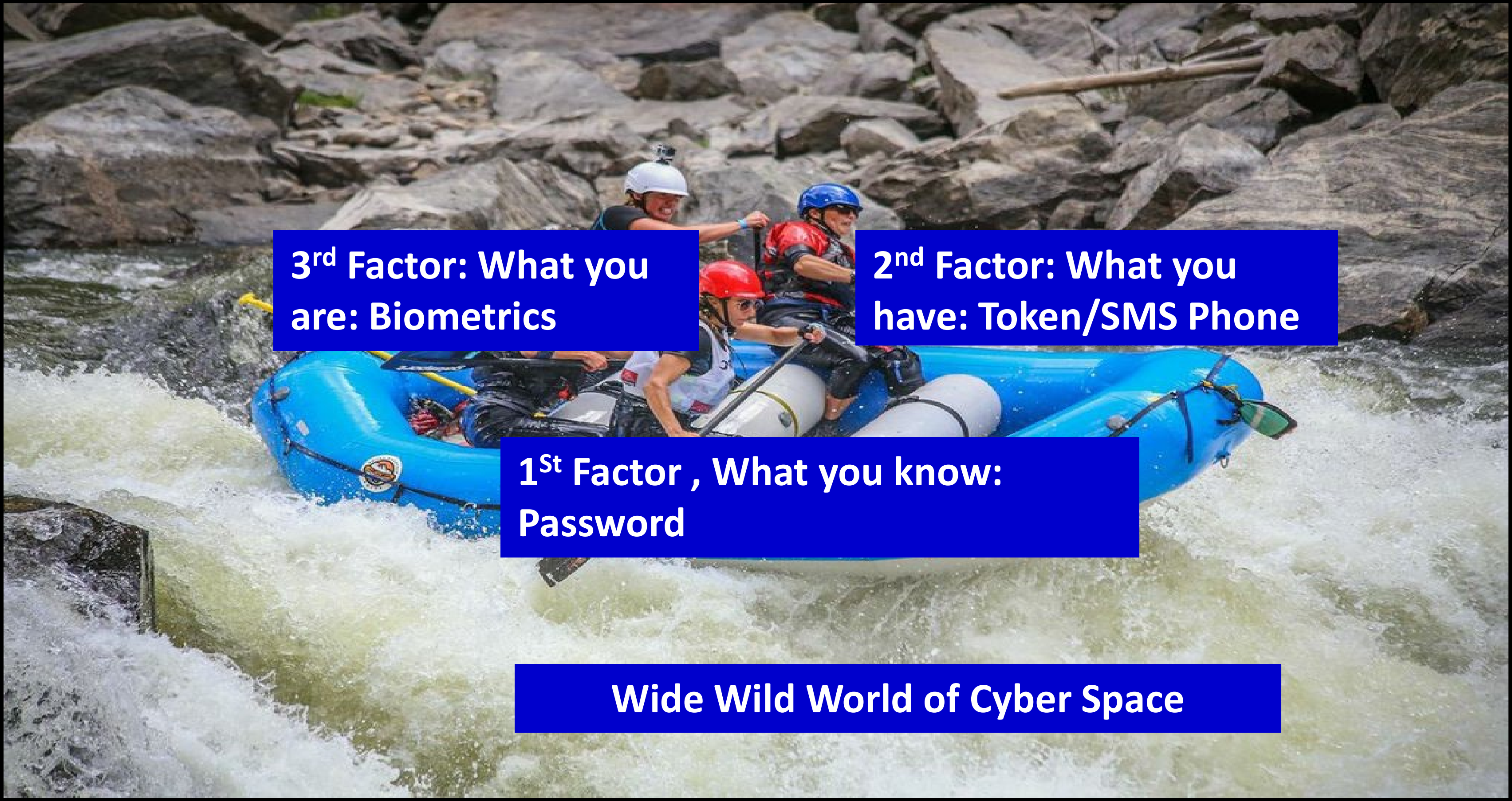
  Wayne Kissinger, Banking Professional


PASSWORDS ARE LIKE
UNDERPANTS
Change them often, keep them private and never share them with anyone.

Multi-Factor Knight!

Method	Examples	Properties
What you know	User Ids, PINs Passwords	Shared Easy to guess Usually forgotten
What you have	Cards Badges Keys	Shared Can be Duplicated Lost or Stolen
Something unique about user	Fingerprint, face, voiceprint, iris scan	Not possible to share Repudiation unlikely Forging difficult Cannot be lost or stolen

Why Choose A Weak Factor (team member)?



3rd Factor: What you are: Biometrics

2nd Factor: What you have: Token/SMS Phone

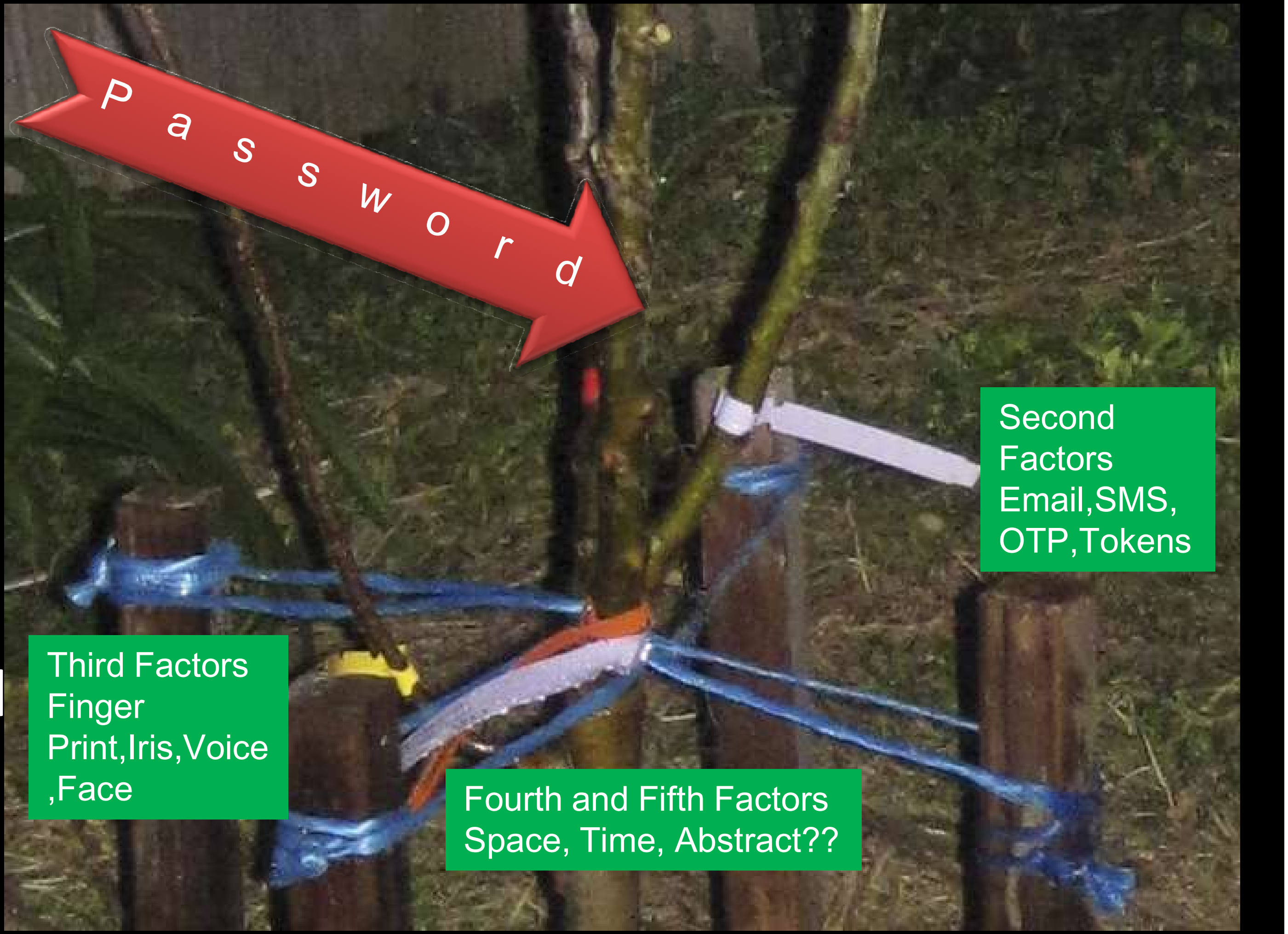
1St Factor , What you know: Password

Wide Wild World of Cyber Space

Strengthen your MFA with <u>ALL Strong Factors</u>

The Multifactor Authentication Frenzy

- To support a weak foundation, need several props
- MFA achieves the same goal



Password

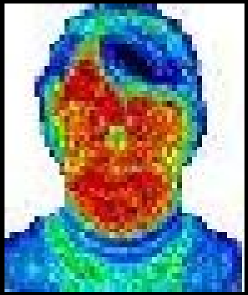
Second Factors Email,SMS, OTP,Tokens

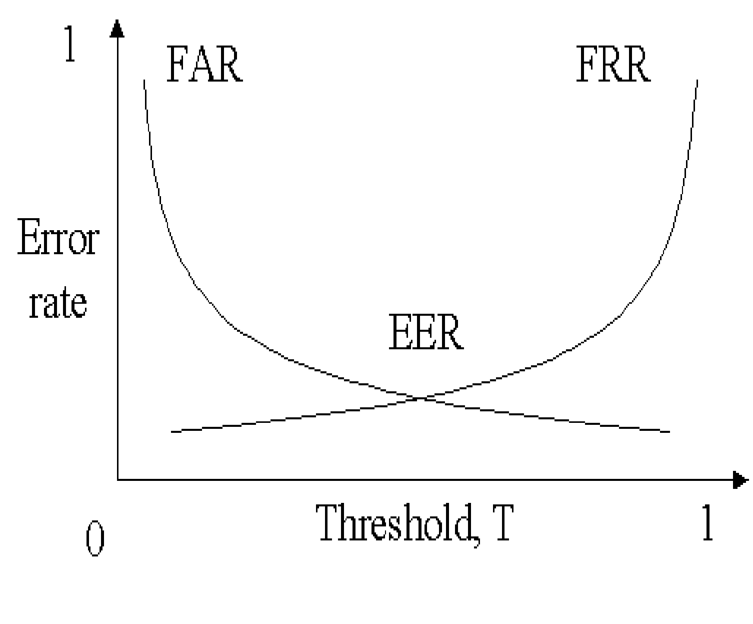
Third Factors Finger Print,Iris,Voice ,Face

Fourth and Fifth Factors Space, Time, Abstract??

Biometrics

Face, Finger, Iris, Palm, Retina, Signature, Voice





FAR: False Acceptance Rate
FRR: False Rejection Rate
EER (also Cross-over): Equal Error Rate

Comparison

Biometric Type	Accuracy	Ease of Use	User Acceptance
Fingerprint	High	Medium	High (if device local) ; Low
Hand Geometry	Medium	High	Medium
Voice	Medium	High	High
Retina	High	Low	Low
Iris	Medium	Medium	Medium
Signature	Medium	Medium	High
Face	Low	High	High

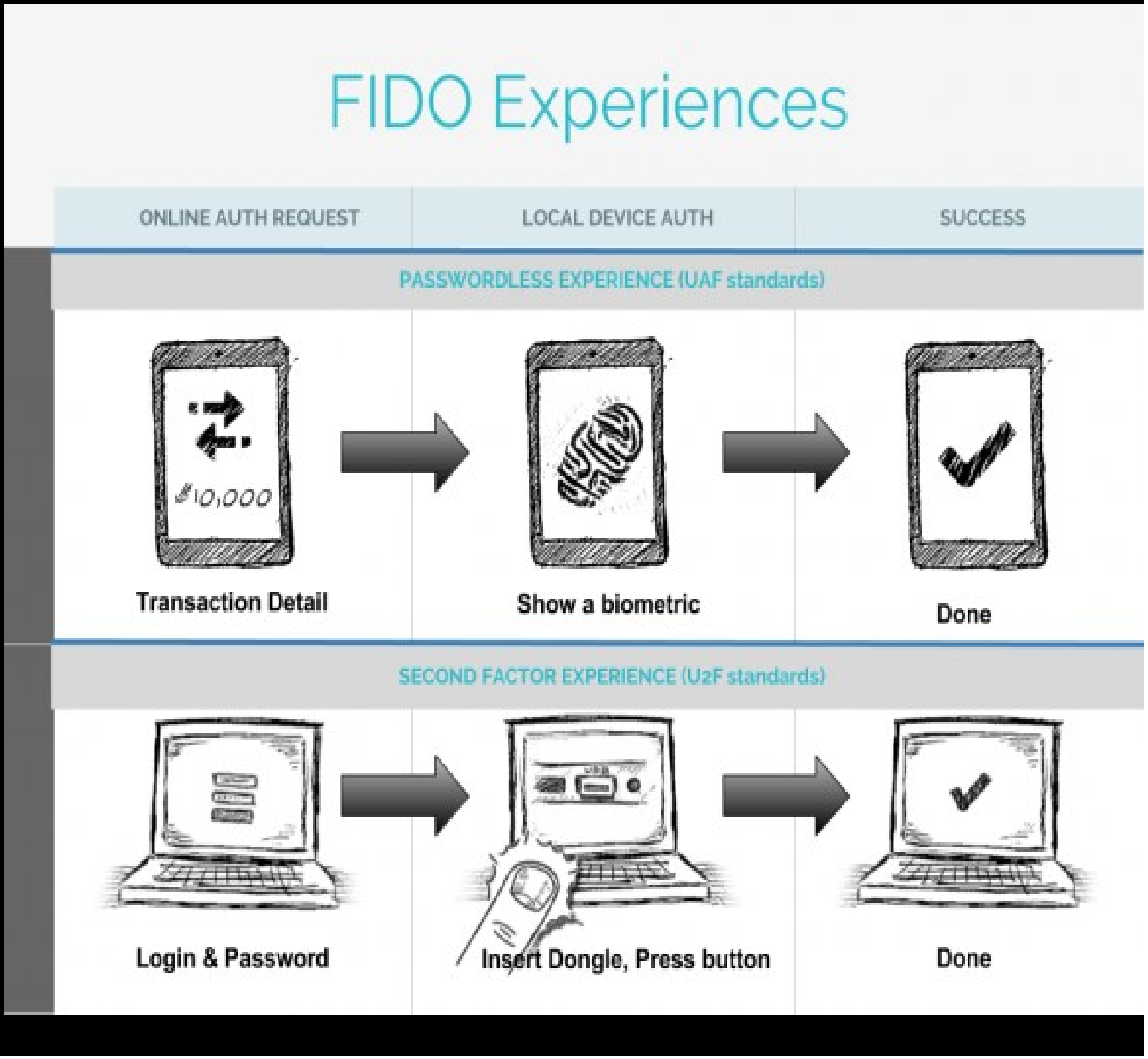
Fast Identity Online (FIDO): UAF and U2F

Universal Access Factor

- Local device authentication (agent)
- Cloud application needs to trust the result of UAF agent on local device

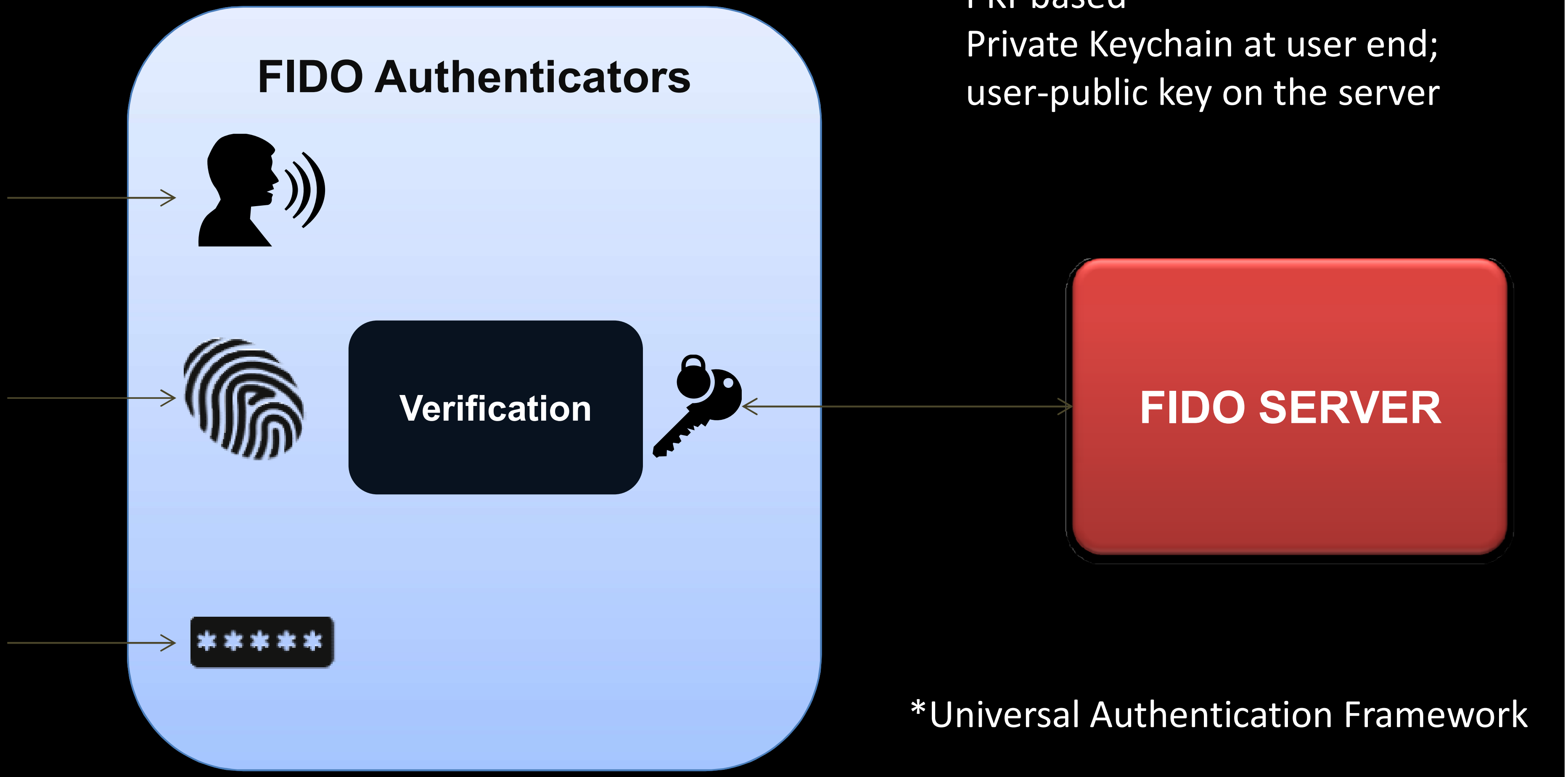
U2F

- Still needs a password
- Either USB Key chain or Bluetooth (others evolving)



How does FIDO UAF* work?

PKI-based
Private Keychain at user end;
user-public key on the server



FIDO Authenticators

Verification

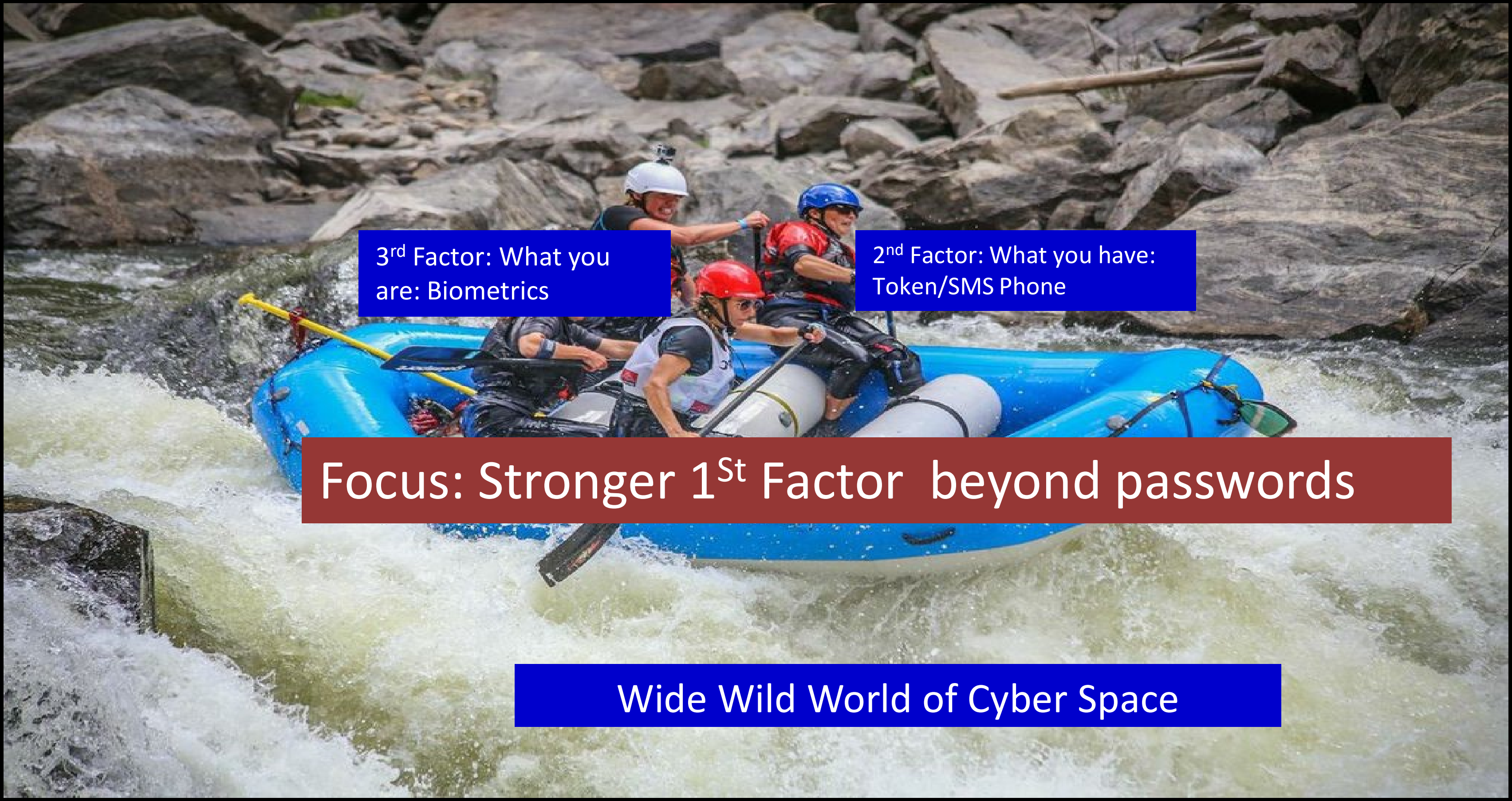
FIDO SERVER

*Universal Authentication Framework

FIDO –Potential issues

- U2F is not zero footprint
- Transaction challenge is still cumbersome
- Even though there is provision on formulating policies over which devices and UAF/U2F, FIDO server accepts
  - Untrusted User Agent
  - Responsibility lies with server to determine unknown risks at user end
- If server is compromised, could replace the public keys for the users (denial of service)
  - No additional public key validation to trust beyond bootstrapped registration
- Device lost – is painful ; all keys are tied in
  - Similar to forgot password flow (traditionally the weakest link)

Can we Do better Than Passwords for 1st Factor?



3rd Factor: What you are: Biometrics

2nd Factor: What you have: Token/SMS Phone

Focus: Stronger 1St Factor beyond passwords

Wide Wild World of Cyber Space

Closer Look At First Factor Authentication

- First Factor only implies “What you know”
    - » Not necessarily ≠ “PASSWORD”
- User response Can be dynamic (changing)
- No additional gadgets needed! – All in the brain
- Cannot be revealed until User chooses to
    - » Willingly or Otherwise
    - – Independently and uniquely can be chosen by the User
    - – Typically depends on other technologies for Mutual Authentication
        - Need not be!

Why First-Factor (knowledge) is indispensable?

- Knowledge-base cost $0 capex
- Zero-footprint - Nothing to carry around or maintain –all in the brain

- •Convenient
- •Still do not have confidence in “what you have” and “what you are” –Absolutely not fool-proof

- Note: First factor always ≠ Password
- First factor merely says “What you know”
  - – How you do
  - – What you do

Optional

Simple Hybrid-Zero-Knowledge Processing (SHZKPP)

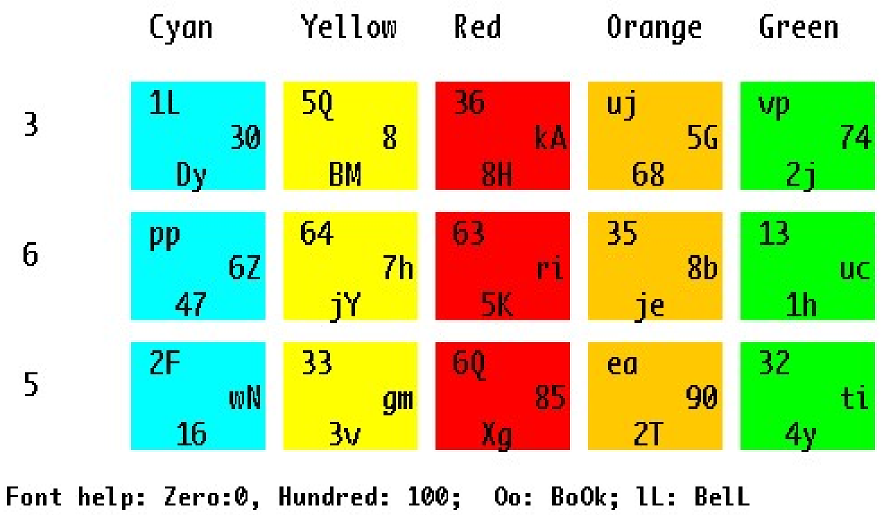
A **zero-knowledge password proof** (ZKPP) is an interactive method for one party (the prover) to prove to another party (the verifier) that it knows a value of a password, without revealing password to the verifier

ZKPP is defined in IEEE 1363.2 as "An interactive zero knowledge proof of knowledge of password-derived data shared between a prover and the corresponding verifier."

Why Simple & Hybrid (explicit and implicit secrets) ZKPP ?

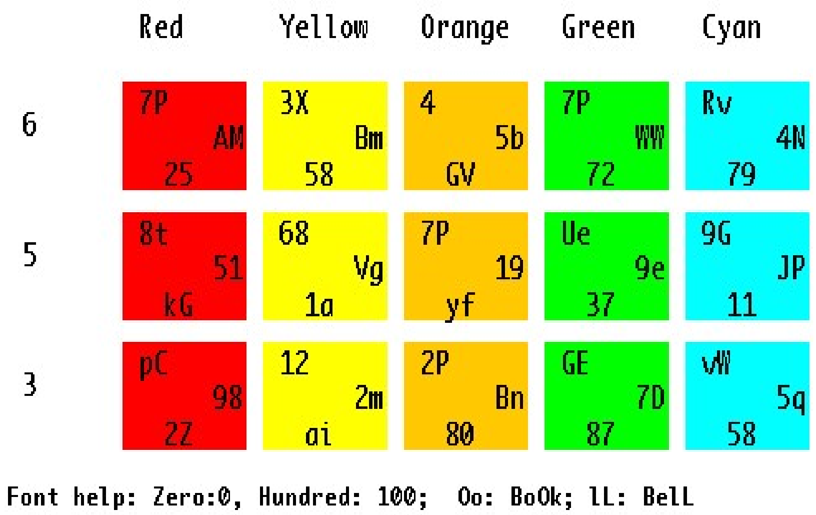
- Zero-footprint –Practically what humans can do
- Retain password user-experience

How does it work?



	Cyan	Yellow	Red	Orange	Green
3	1L 30 Dy	5Q 8 BM	36 kA 8H	uj 5G 68	vp 74 2j
6	pp 6Z 47	64 7h jY	63 ri 5K	35 8b je	13 uc 1h
5	2F wN 16	33 gm 3v	6Q 85 Xg	ea 90 2T	32 ti 4y

Font help: Zero:0, Hundred: 100; Oo: BoOk; lL: BelL



	Red	Yellow	Orange	Green	Cyan
6	7P AM 25	3X Bm 58	4 5b GV	7P WW 72	Rv 4N 79
5	8t 51 kG	68 Vg 1a	7P 19 yf	Ue 9e 37	9G JP 11
3	pC 98 2Z	12 2m ai	2P Bn 80	GE 7D 87	vW 5q 58

Font help: Zero:0, Hundred: 100; Oo: BoOk; lL: BelL

Answer: 43

process

OTP: jjetw427$2&dse+@

+ Shared secret1 (txt)

Answer: 48

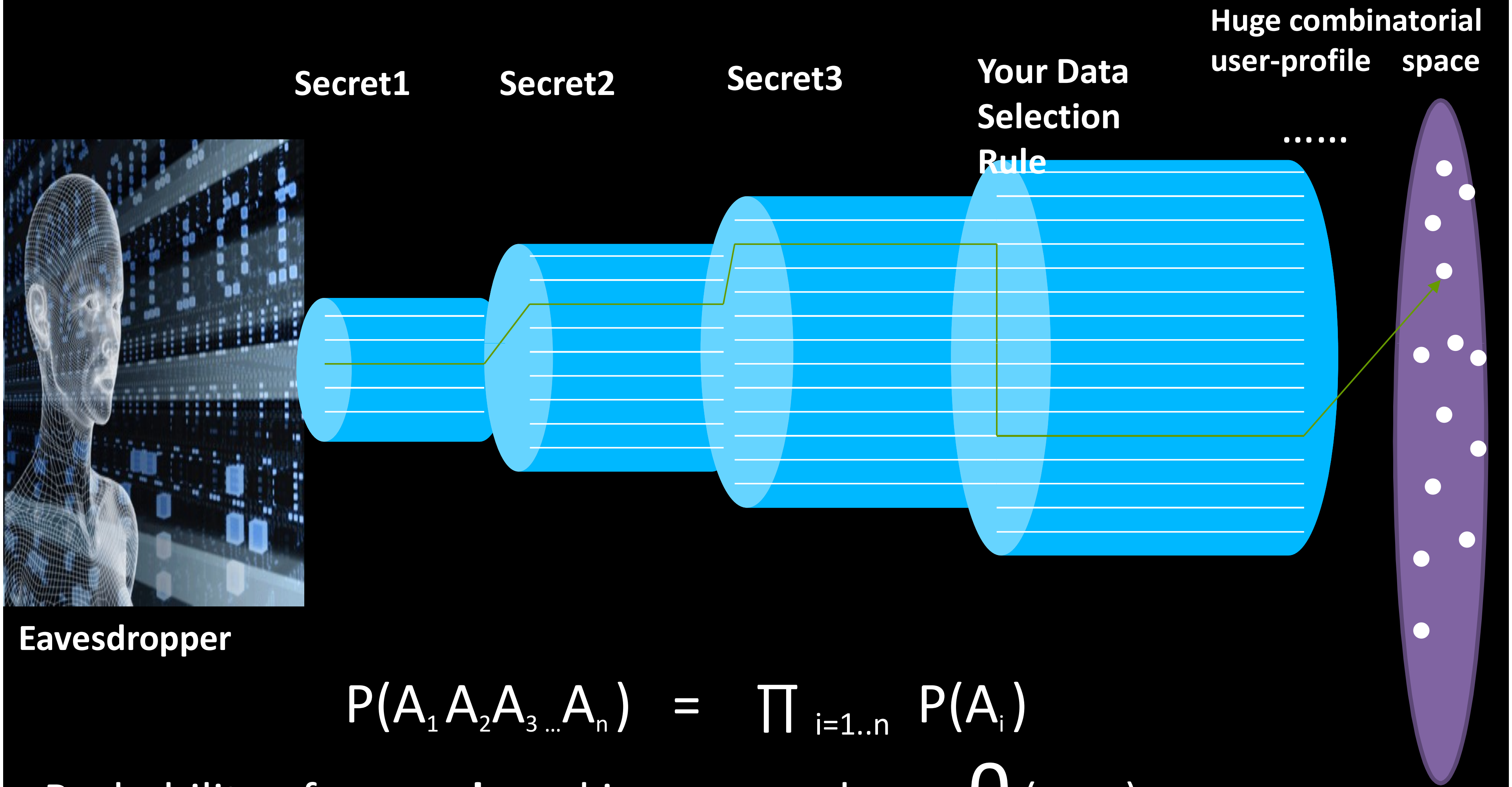
process

OTP: dj,ey12c4r844#f

+Shared secret2 (txt)

Two different challenge instances of one user account

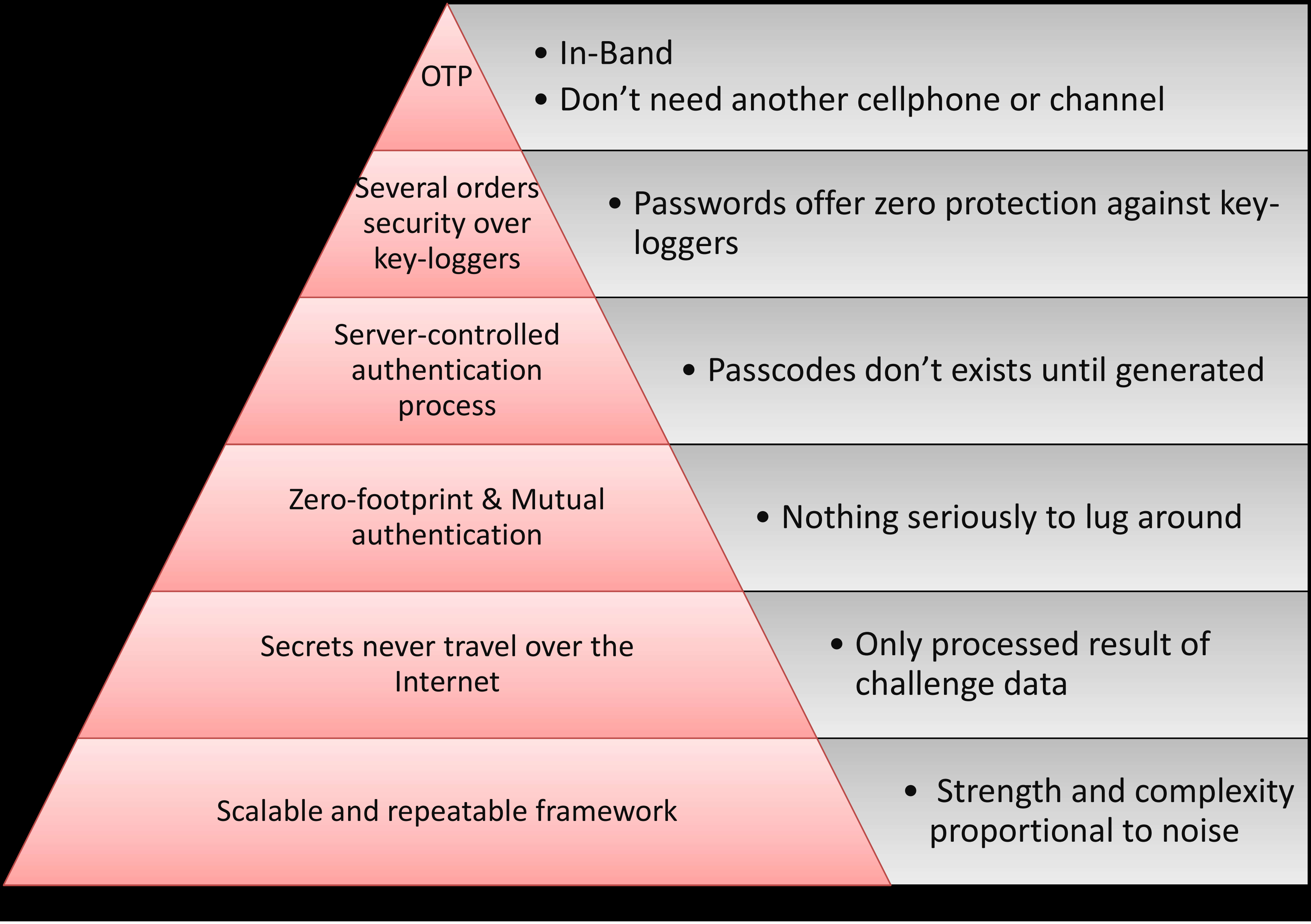
Reverse-Turing Test-based & Probability



$$P(A_1 A_2 A_3 \ldots A_n) = \prod_{i=1..n} P(A_i)$$

Probability of **manual** cracking approaches ~ 0 (zero)

Key Highlights of the SHZKPP schemes



OTP

- In-Band
- Don’t need another cellphone or channel

Several orders security over key-loggers

- Passwords offer zero protection against key-loggers

Server-controlled authentication process

- Passcodes don’t exists until generated

Zero-footprint & Mutual authentication

- Nothing seriously to lug around

Secrets never travel over the Internet

- Only processed result of challenge data

Scalable and repeatable framework

- Strength and complexity proportional to noise

Containing Credential Explosion: Single-Sign On (SSO)

- As number of protected applications increase ~ # Passwords also increase
- Average need of around 20 passwords in day-to-day life
- Humans can at best remember 6 secrets

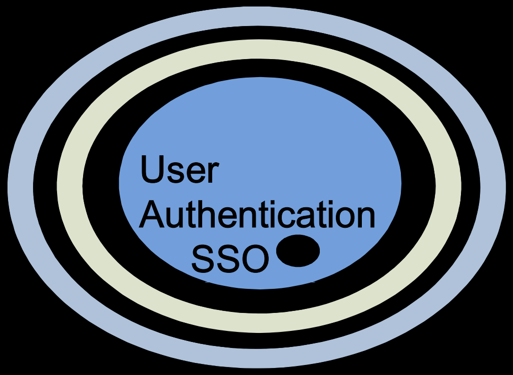
Within Enterprise SSO and across Enterprises (Federated SSO)

Major Mechanisms of SSO

	OpenID	**OAuth**	**SAML**	**OpenID Connect**
Dates from	2007	2006	2002	2010
Current version	OpenID 2.0	OAuth 2.0	SAML 2.0	OpenID Connect 1.0 (new)
Main purpose	Single sign-on for consumers	API authorization between applications	Single sign-on for enterprise users	Combine OpenID authentication identifcation and Oauth authorization
Protocols used	XRDS, HTTP	JSON, HTTP	SAM, XML, HTTP, SOAP	JSON, HTTP

Summary

- Passwords the frontline authentication mechanism is fragile
  - Many hacks and attacks – almost a broken technology
- Second and Third factor authentication mechanisms depend either on carrying a gadget or susceptible to errors –technology advances improving



- Zero-footprint dynamic disposable passcodes can balance the complexity and scalability while retaining password experience
  - SSO further reduces the need to multiple credentials
- As ever, layered approach with compensating controls suggested

Q & A? Thank you!

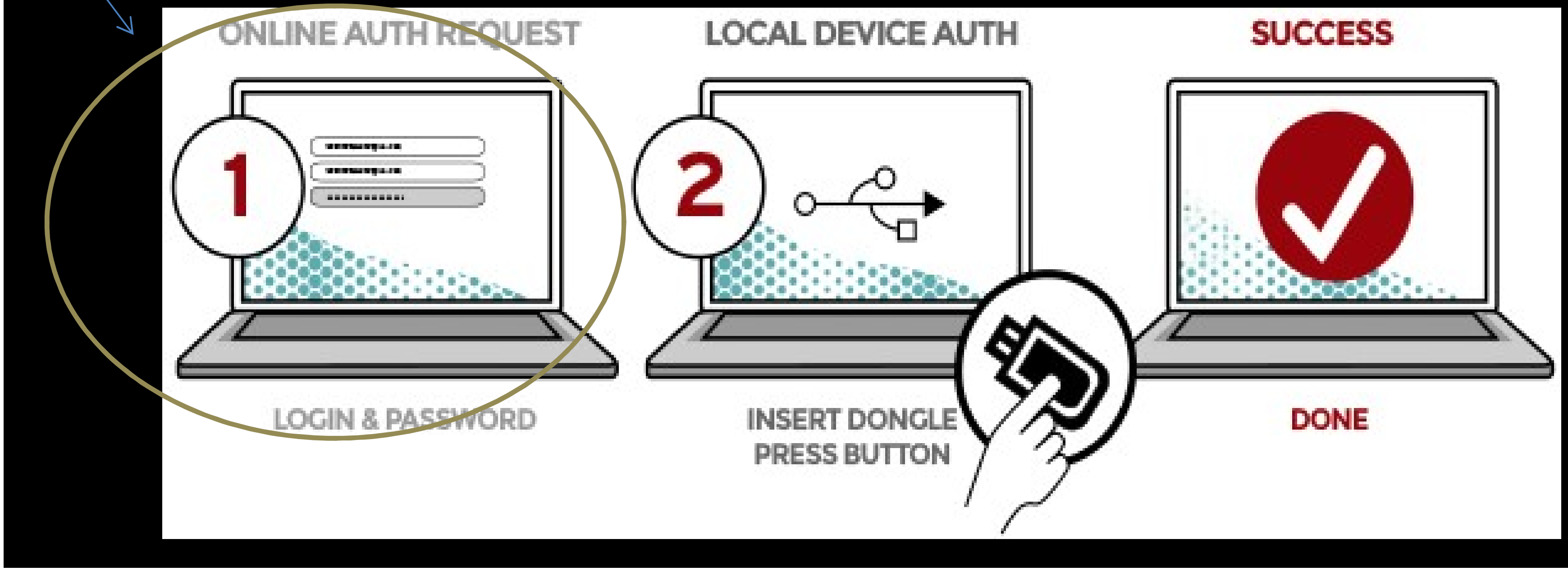
FIDO: Universal Second Factor - U2F

U2F is an open 2-factor authentication standard enables

- keychain devices, mobile phones and other devices
- securely access any number of web-based services

The U2F specifications are today hosted by the FIDO Alliance (http://fidoalliance.org/specifications/download)

Passwords!



Quick Lingo

SAML

- Assertion
  - Data by vouching authority on authentication or any attribute of the user including authorization scope of a resource
- Binding
  - Mapping of elements from protocol1 to protocol2
- Profiles
  - A set of rules usage of assertions or protocol messages usage or mapping of attributes

Oauth

- Tokens

– Access tokens are credentials used to access protected resources; similarly refresh tokens are credential used to get access token to access a resource

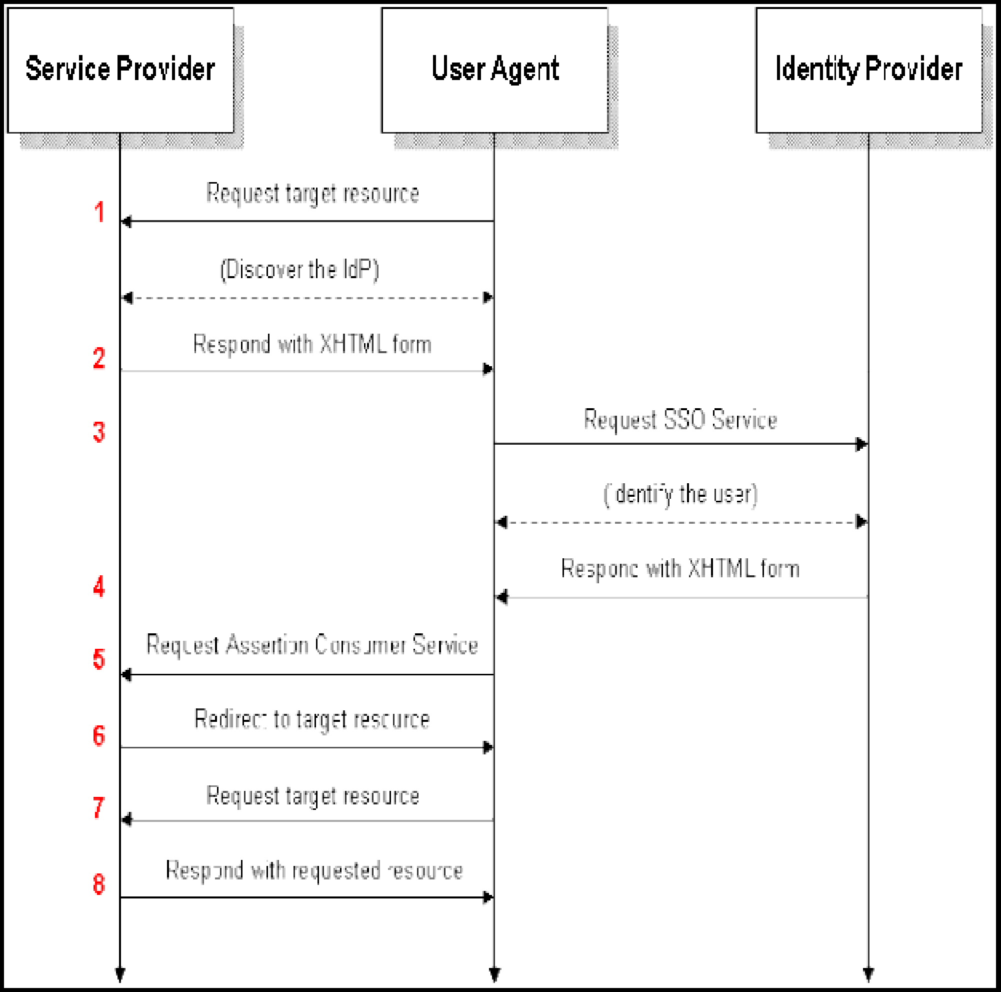
- Authorization grant

– After verification of user credentials and consent of resource utilization issued authorization grant

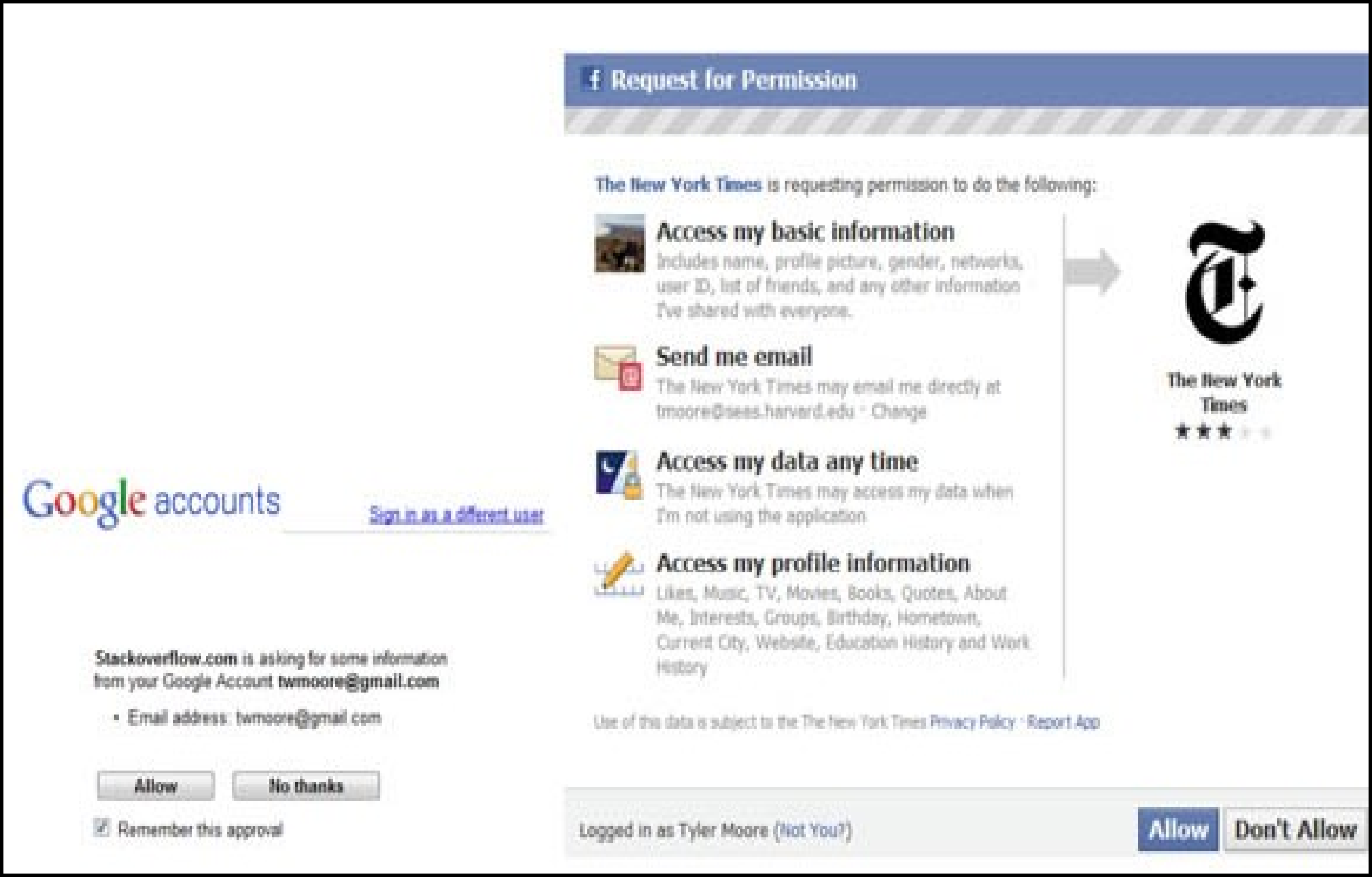
- Resource
  - A protected resource for which access it requested.

SAML 2.0 – Web SSO Protocol

- Service provider generates a SAML request and redirects to IDP
- IDP authenticates and asserts user profile and issues SAML token
- Service provider grants access to resource after verification



OAuth example



Google accounts

Sign in as a different user

Stackoverflow.com is asking for some information from your Google Account **twmoore@gmail.com**

- Email address: twmoore@gmail.com

Allow | No thanks

☑ Remember this approval

Request for Permission

The New York Times is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

Send me email
The New York Times may email me directly at tmoore@seas.harvard.edu · Change

Access my data any time
The New York Times may access my data when I'm not using the application

Access my profile information
Likes, Music, TV, Movies, Books, Quotes, About Me, Interests, Groups, Birthday, Hometown, Current City, Website, Education History and Work History

The New York Times
★★★☆☆

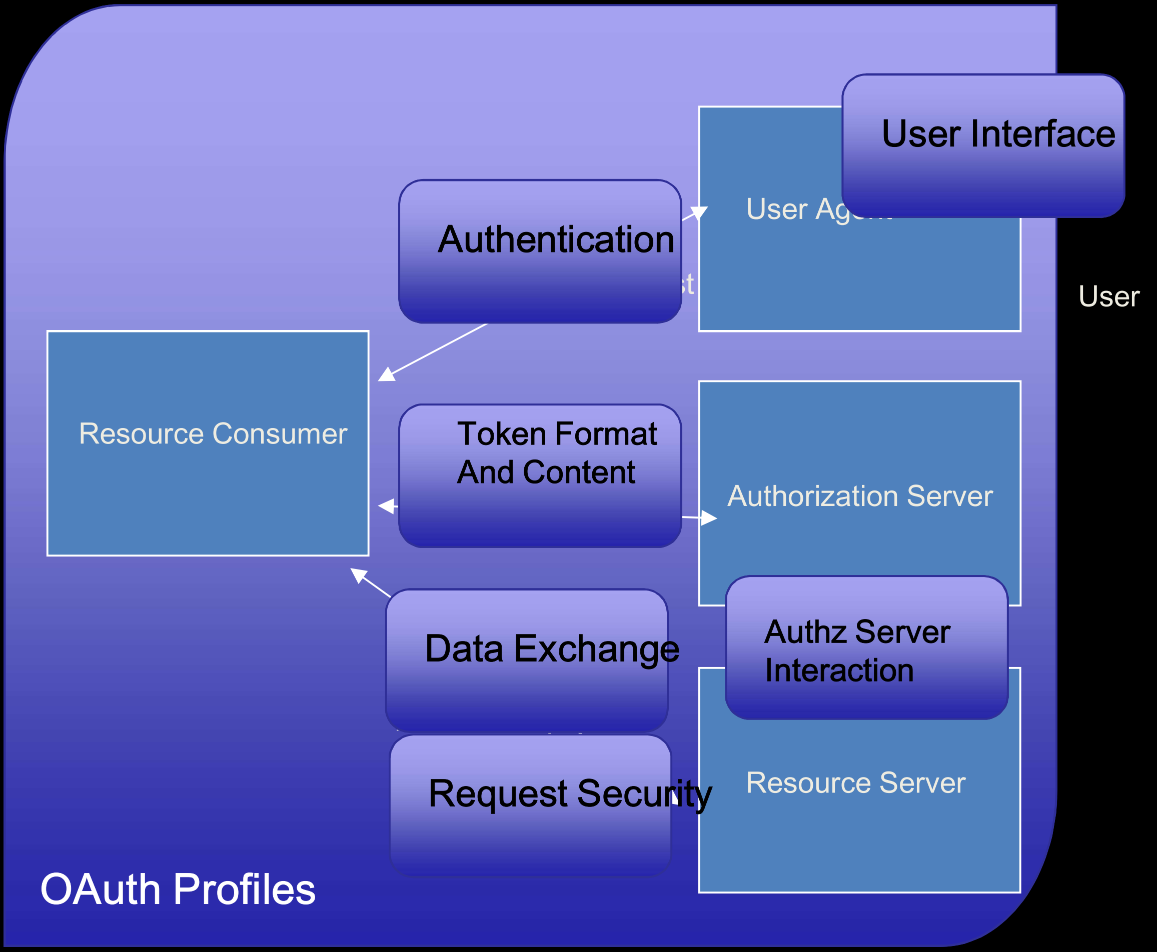
Use of this data is subject to the The New York Times Privacy Policy · Report App

Logged in as Tyler Moore (Not You?)

Allow | Don't Allow

Oauth 2 Flow

- Resource request translates into authentication and authorization and access token
- Resource consumer can use the resource until token expires
- Can be refreshed or reissued depending on policy


User Interface
User Ag
Authentication
User
Resource Consumer
Token Format
And Content
Authorization Server
Data Exchange
Authz Server
Interaction
Request Security
Resource Server
OAuth Profiles