KnowBe4
Human error. Conquered.

Hacking Biometrics:

If You Thought Your Fingerprints Were Safe, Think Again

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

e: rogerg@knowbe4.com
Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

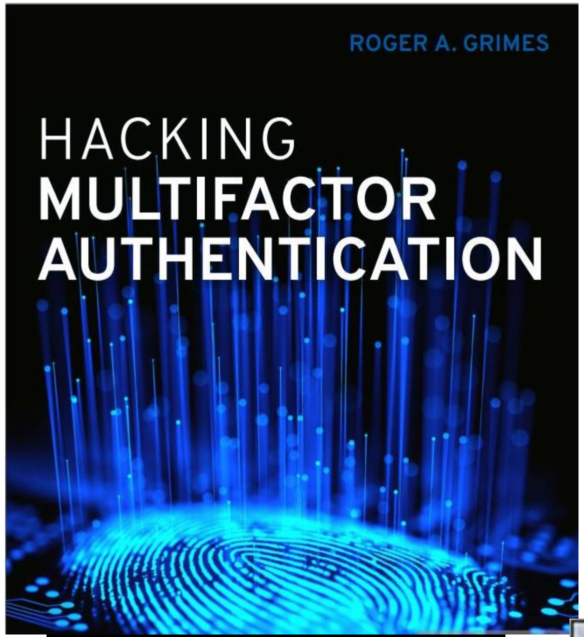
About Roger

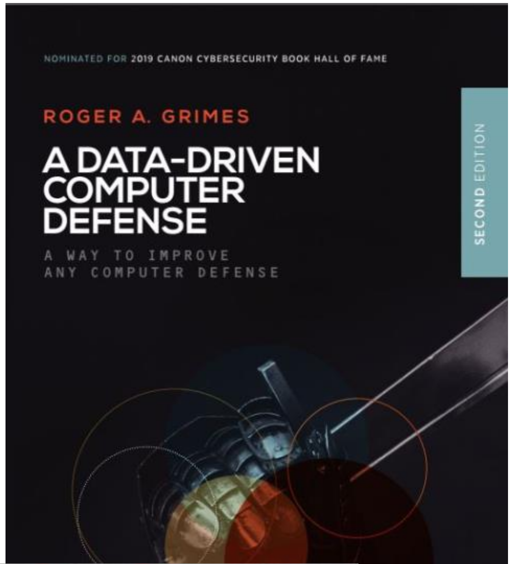
- 34 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 13 books and over 1,200 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

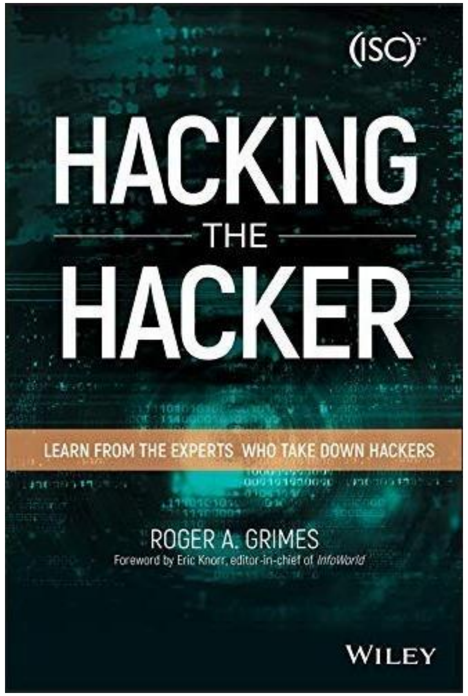
Certification exams passed include:

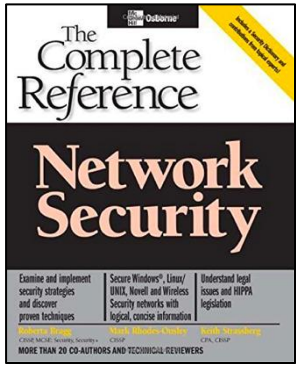
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

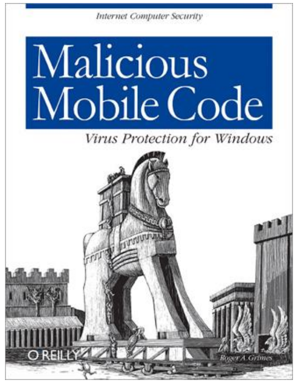
Roger’s Books

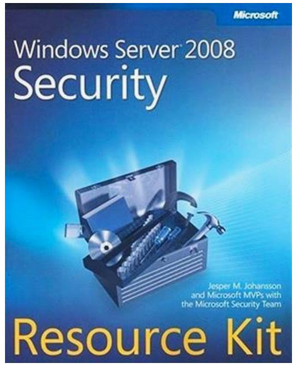


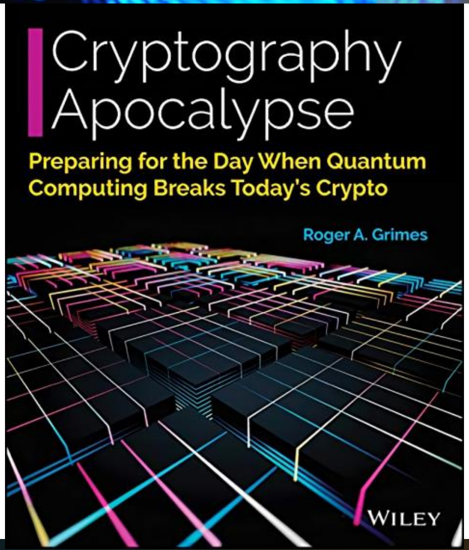


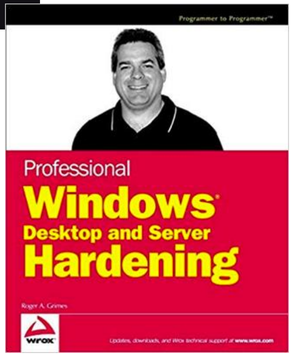

(ISC)²
HACKING
THE
HACKER
LEARN FROM THE EXPERTS WHO TAKE DOWN HACKERS
ROGER A. GRIMES
Foreword by Eric Knorr, editor-in-chief of InfoWorld
WILEY

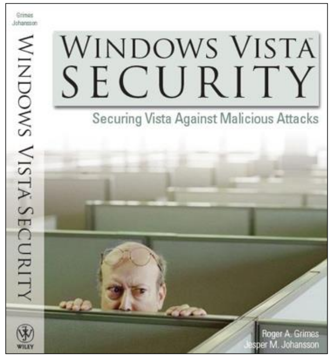


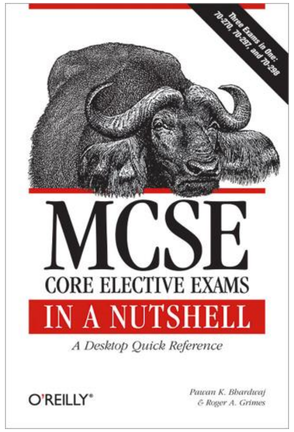


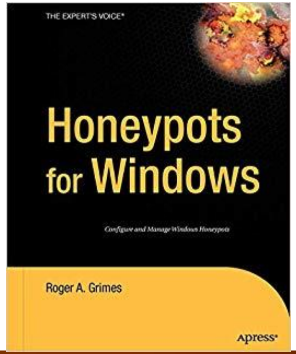



Cryptography
Apocalypse
Preparing for the Day When Quantum
Computing Breaks Today’s Crypto
Roger A. Grimes
WILEY









About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, Norway, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

FORRESTER®

WAVE LEADER 2022

Security Awareness And Training Solutions

TRAIN
PHISH
ANALYZE

AMERICA'S FASTEST-GROWING PRIVATE COMPANIES

Inc. 500

Gartner peerinsights customers' choice 2021 ™

Agenda

- Biometric Basics
- Hacking Biometrics
- Safer Biometrics

Agenda

- Biometric Basics
- Hacking Biometrics
- Safer Biometrics

Biometric Basics

Biometric attributes are used to authenticate people in digital systems

Common Types:

- Fingerprints, face, retina, iris, palm, geometry, veins, voice, touchless, etc.
- Behavioral: typing (keystroke dynamics), cursor movements, etc.
- Experimental: Smell, brainprint, etc.
- DNA the ultimate??

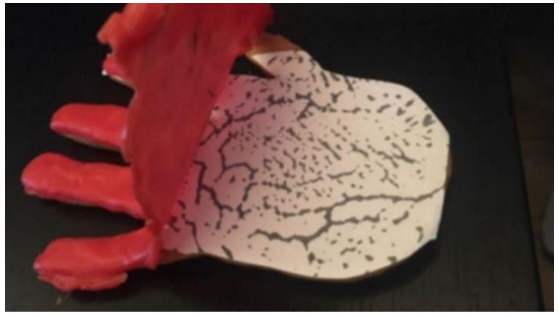
- Can be used 1FA or MFA

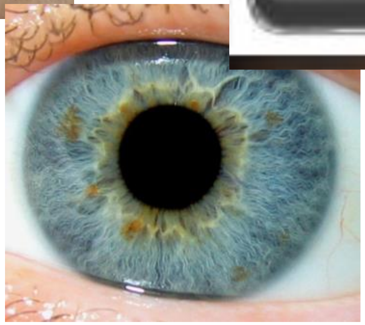
Biometric Basics

Why Are Biometrics Used?

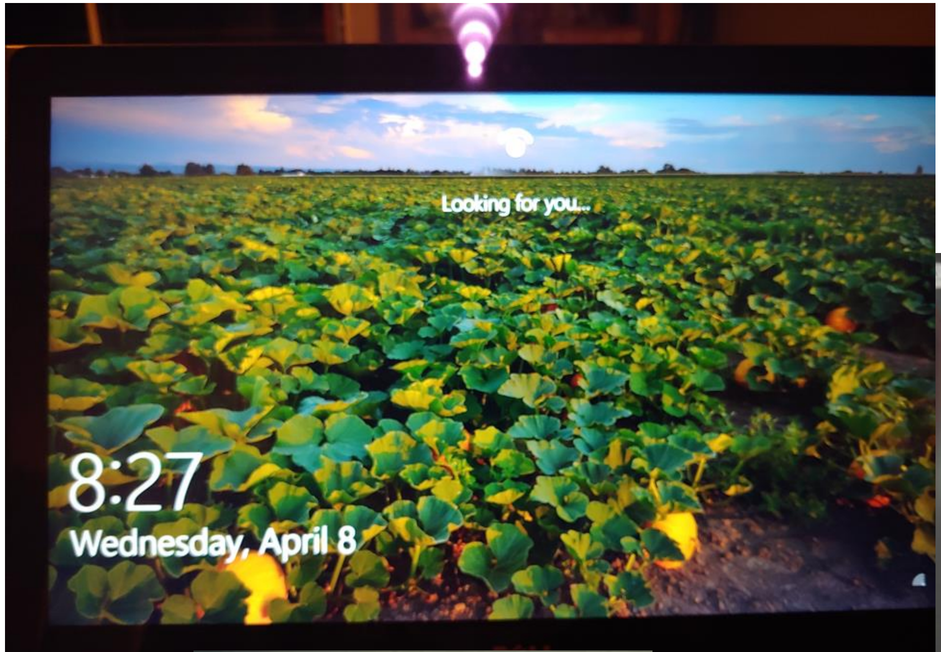
- Always on you
- Supposedly universally unique or darn close anyway
- Measured attributes usually change slowly over time for most people
- Can be measured quickly

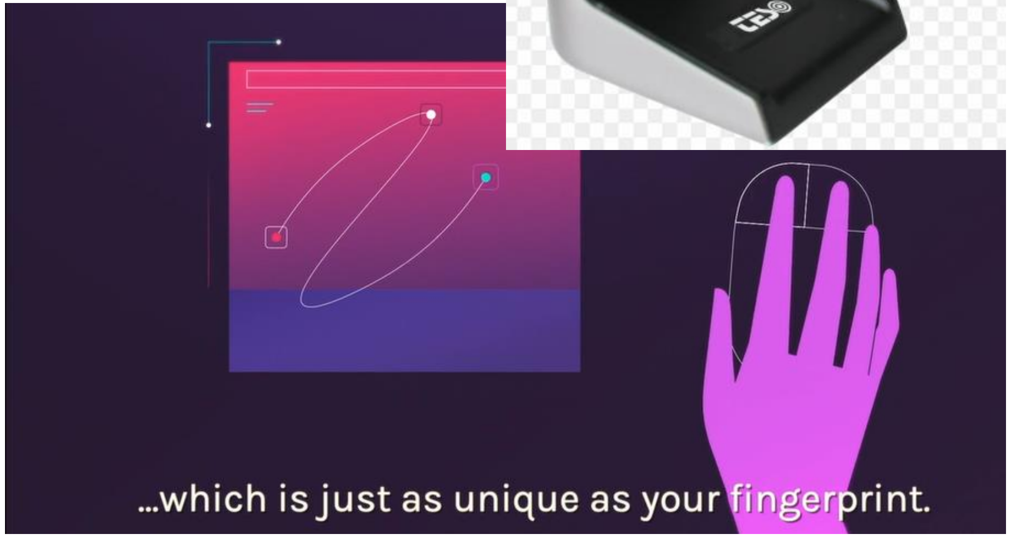
Biometric Basics

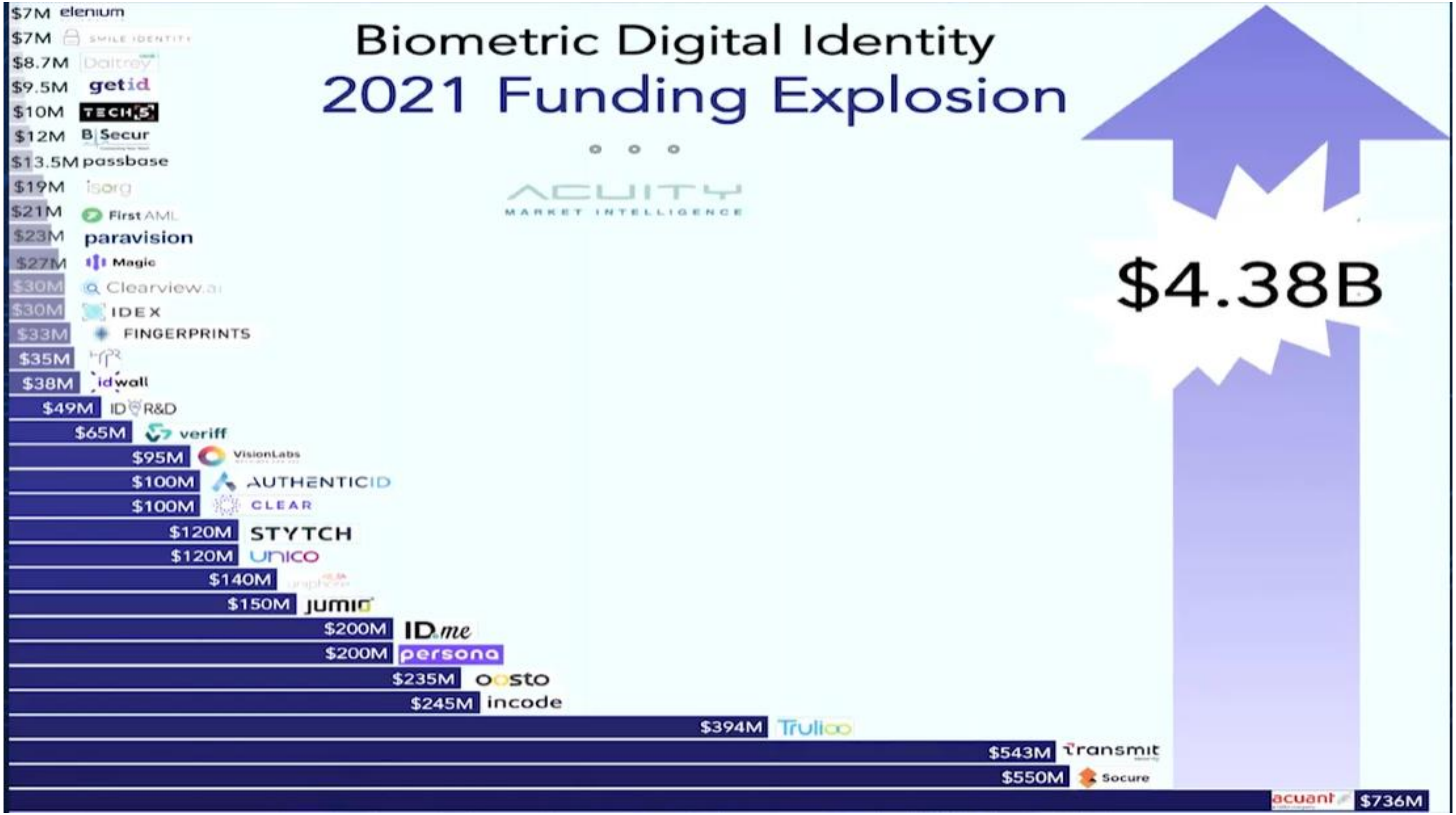




Biometric Basics







https://www.acuitymi.com/post/the-2021-biometric-digital-identity-investment-explosion

Biometric Basics

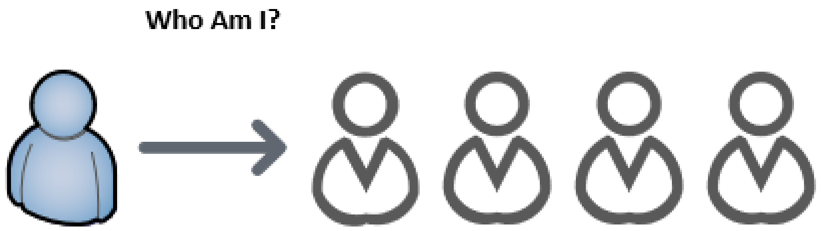
- Some biometric solutions are great and accurate
- Many aren’t
- Most are not as accurate as believed by customer
- Most are not as accurate as claimed by vendor

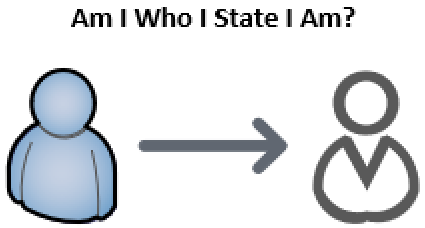
- All can be hacked
- But anything can be hacked…including biometrics
- Some biometric solutions are far more resilient than others

Biometric Basics

Biometric systems are generally set to one of two id modes:

- **One-to-many (1:N)**
  - Compare submission to large group to find one person, **<u>identification</u>**
- **One-to-one (1:1)**
  - Ex. Using your fingerprint to logon to your phone, **<u>verification</u>**



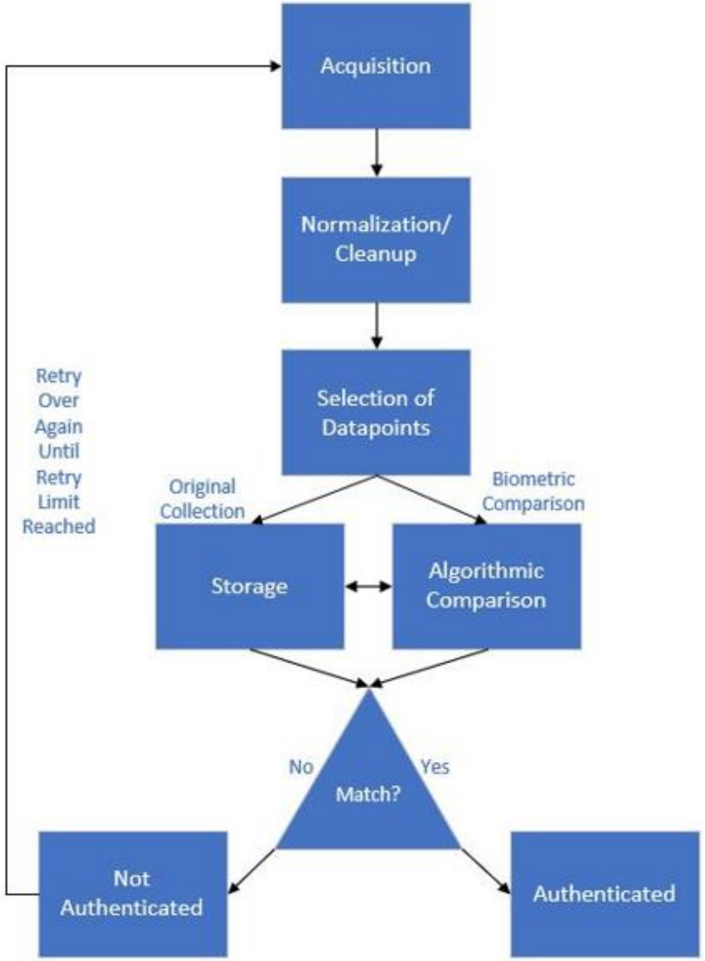


- Generally, one-to-one mode is easier

Biometric Basics

Basic Process

- Capture
- Storage
- Usage



From Chapter 16 of Hacking Multifactor Authentication book

Biometric Basics

Problem Summary

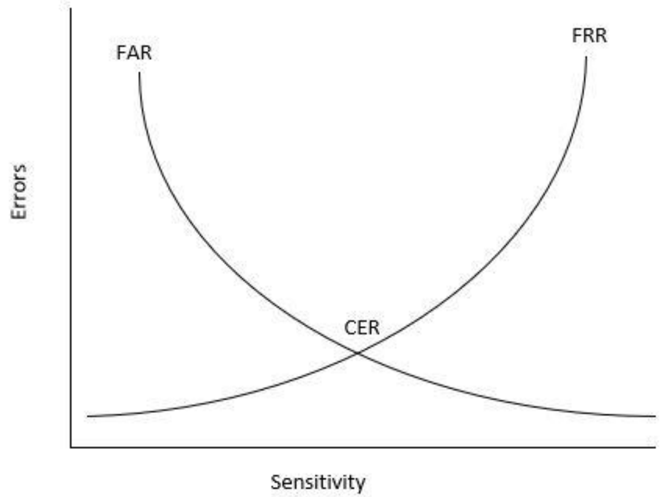
- Accuracy
- Security/Hacking
- What to do if biometric attribute stolen?
- Shared systems can promote disease transmission
- Privacy issues, government intrusion, etc.
- Bias

Biometric Basics

Problems

Accuracy

- Biometrics can have a high number of:
  - False-Negatives/False Reject Rate (Type I error)
  - False-Positives/False Accept Rate (Type II error)
  - Cross-Over Error Rate (CER)

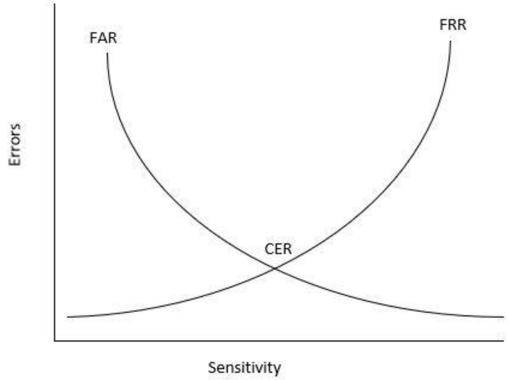


Biometric Basics

Problems

Accuracy

- What Everyone Wants: Low number of false-negatives and false-positives
  - But, in most cases, as you lower false-negatives you raise false-positives and vice-versa
  - In general, if you have to make a trade-off:
    - Want low false-negatives for verification
    - Want low false-positives for identification



Biometric Basics

Problems - Accuracy

Edge Cases - Some people can never use a particular biometric solution

- People born without fingers, eyes, mute, etc.
- Biological dupes may exist (i.e., twins, etc.)
- Eye diseases cause constant change
- Adermatoglyphia – born without fingerprints
- Facial hair changes, new scars, tattoos, weight gain, etc.
- Play guitar, work with abrasive materials, paint, garden, etc.
- Glasses, masks, lighting, angles, etc., undermine accuracy

Biometric Basics

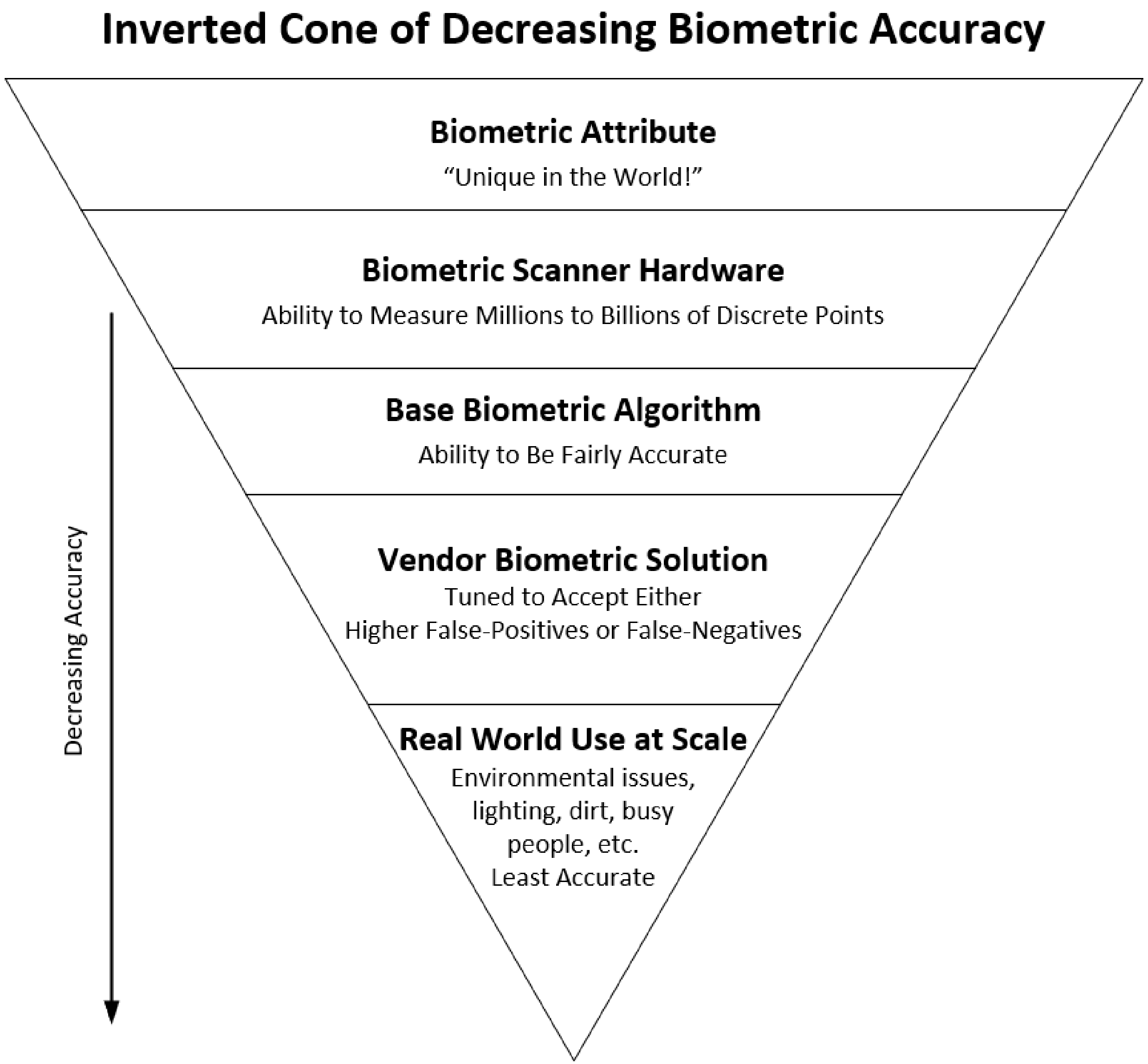
Problems

Accuracy

- Some/most vendors claimed accuracy rates are suspect
    - They will tell you how the biometric attribute involved, itself, is “unique in the world”
    - They will tout the involved hardware’s “great” potential accuracy rate
    - They will point to the theoretical boundaries of what their solution is capable of

    - But the only accuracy you should care about is the solution’s complete, end-to-end, accuracy as used in the real world

Biometric Basics



Inverted Cone of Decreasing Biometric Accuracy

Biometric Attribute
"Unique in the World!"

Biometric Scanner Hardware
Ability to Measure Millions to Billions of Discrete Points

Base Biometric Algorithm
Ability to Be Fairly Accurate

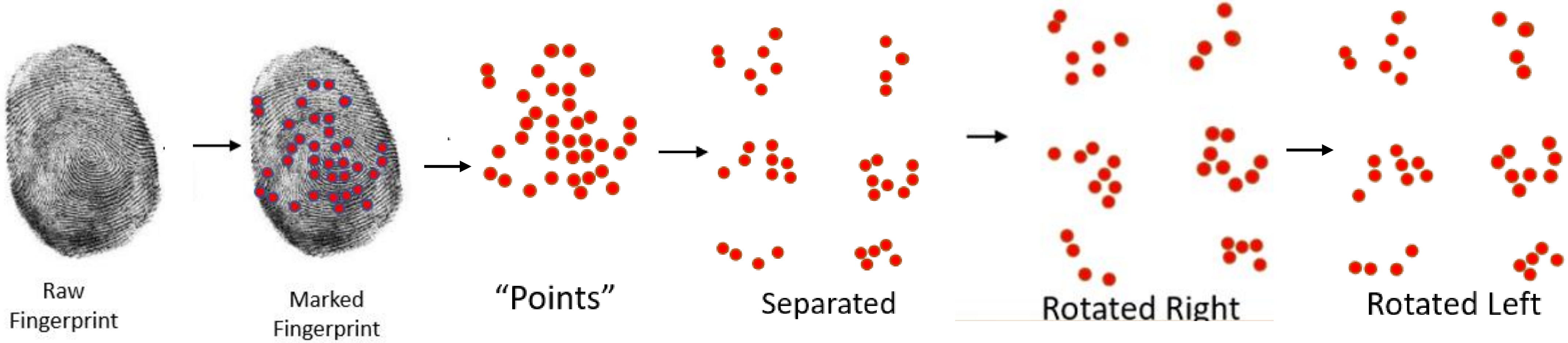
Vendor Biometric Solution
Tuned to Accept Either
Higher False-Positives or False-Negatives

Real World Use at Scale
Environmental issues,
lighting, dirt, busy
people, etc.
Least Accurate

Biometric Basics

Accuracy –Example: Fingerprints

- “Your fingerprints are unique in the world!”
- Likely a true statement, but we aren’t even sure about that



What is actually stored and used is far less unique in the world

Biometric Basics

Accuracy –Example: De-Tuning

- Biometric readers in most popular consumer devices and even in corporate environments are intentionally significantly “detuned” to lower false-negatives
- Because people get mad if the system doesn’t recognize them or if they have to do repeated submissions
- This increases the chances of false-positives significantly

Biometric Basics

Accuracy –Example: Fingerprints

- False-positive fingerprint matches on real-world biometric systems are fairly common
- Example real world: 500-person organization, had:
  - Multiple fingerprint matches among employees
  - Several employees had to use different fingers than first one requested to achieve separation
  - At least 1 employee just couldn’t use the system

Biometric Basics

Accuracy –Example: Fingerprints

- False-positive fingerprint matches on real-world biometric systems are fairly common

Example real world: My cell phone

  - Supposedly the standard is 1:50,000 accuracy
  - My cell phone has been unlocked by a customer’s fingerprints

  Other Examples

  - https://www.cnbc.com/2022/08/26/google-pixel-6a-fingerprint-issue-my-friend-unlocked-my-phone.html
  - https://www.youtube.com/watch?v=RqkydbXgbMA
  - https://www.youtube.com/watch?v=-kflCMQWxiY (around 15:50)

Biometric Basics

Accuracy –Example: Fingerprints

NISTIR 8034

Fingerprint Vendor Technology Evaluation

- December 2014
- The largest study of real-world fingerprint solutions
- https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf
- 733 participants
- **Most accurate "miss rate" was 1.9%**
- **Most solutions were 5%-15%**
- **But in general, fingerprint technology gets better every year**

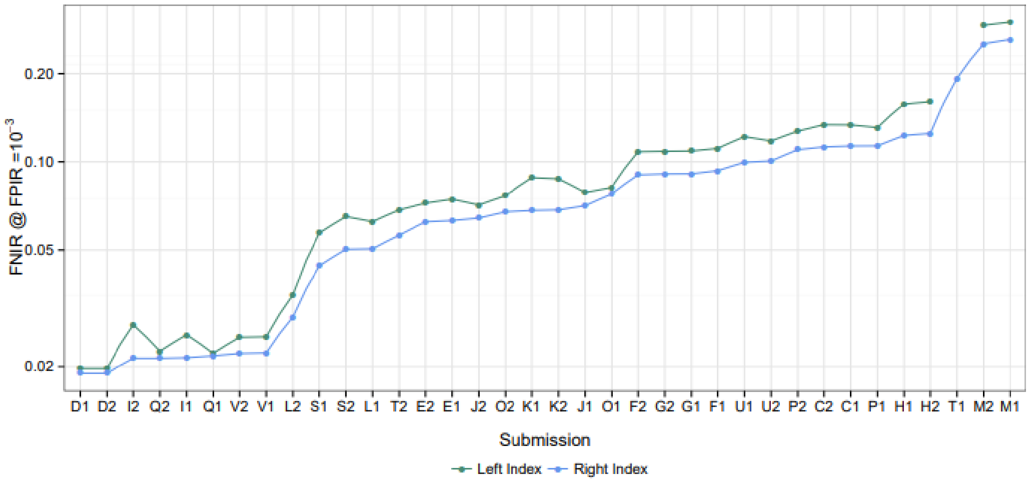
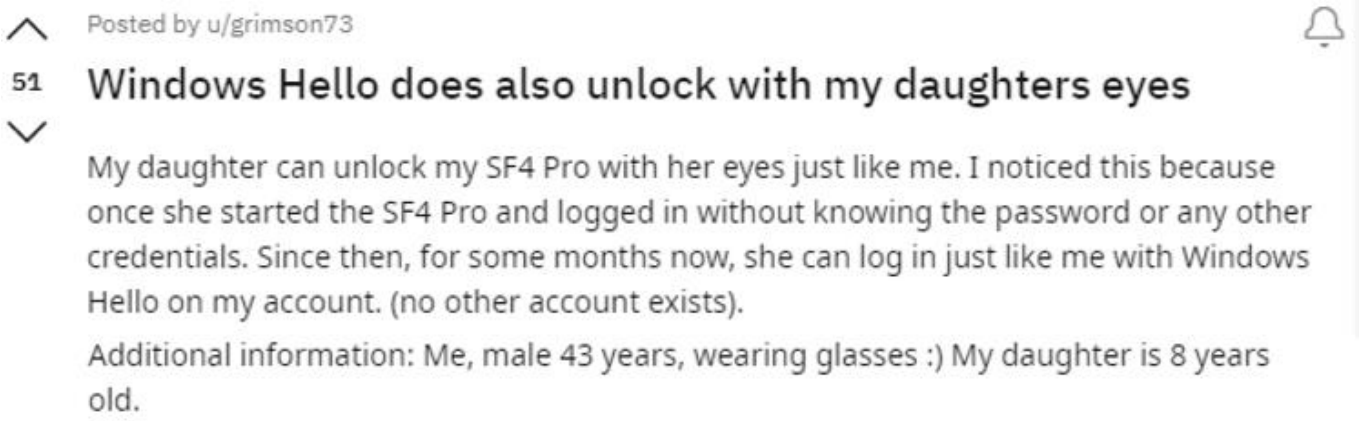


Figure 12: Rank-sorted FNIR @ FPIR $= 10^{-3}$ for Class A — Single Index Finger searching 30 000 subjects against 100 000 subjects. Submissions "1" and "2" from round 3.

Biometric Basics

Accuracy –Example: Windows Hello Facial Recognition

- I’ve had many people over the years email or come up to me to say that Windows Hello logged in their young son or daughter as them, even though they look nothing alike



Posted by u/grimson73

51

Windows Hello does also unlock with my daughters eyes

My daughter can unlock my SF4 Pro with her eyes just like me. I noticed this because once she started the SF4 Pro and logged in without knowing the password or any other credentials. Since then, for some months now, she can log in just like me with Windows Hello on my account. (no other account exists).

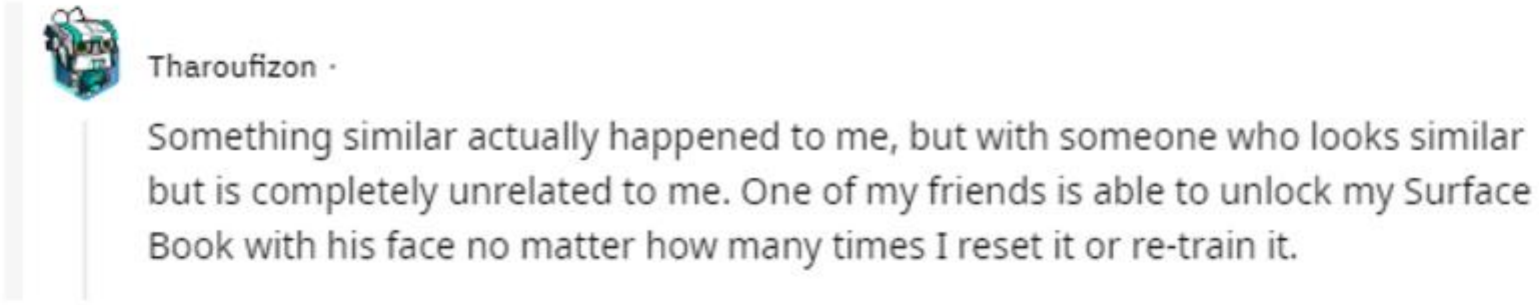
Additional information: Me, male 43 years, wearing glasses :) My daughter is 8 years old.

https://www.reddit.com/r/Surface/comments/5h1zb5/windows_hello_does_also_unlock_with_my_daughters/

Biometric Basics

Accuracy –Example: Windows Hello Facial Recognition

- More stories



Tharoufizon ·

Something similar actually happened to me, but with someone who looks similar but is completely unrelated to me. One of my friends is able to unlock my Surface Book with his face no matter how many times I reset it or re-train it.

https://www.reddit.com/r/Surface/comments/5h1zb5/windows_hello_does_also_unlock_with_my_daughters/

Biometric Basics

Problems

Accuracy

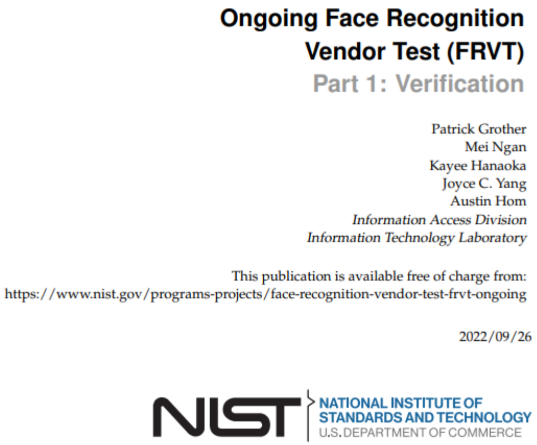
- **NIST Face Recognition Vendor Test (FRVT)** is a multi-year, ongoing evaluation of face recognition algorithms applied to large image databases sequestered at NIST.
- Since 2017, over 450 algorithm applications submitted so far
- https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing
- https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf

Biometric Basics

Problems

Accuracy

- **A “false non-match rate” or FNMR is the rate at which a biometric solution says the same person is not the same person**



Ongoing Face Recognition
Vendor Test (FRVT)
Part 1: Verification

Patrick Grother
Mei Ngan
Kayee Hanaoka
Joyce C. Yang
Austin Hom
Information Access Division
Information Technology Laboratory

This publication is available free of charge from:
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

2022/09/26

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Biometric Basics

1.0 = 100%, Lower numbers are better

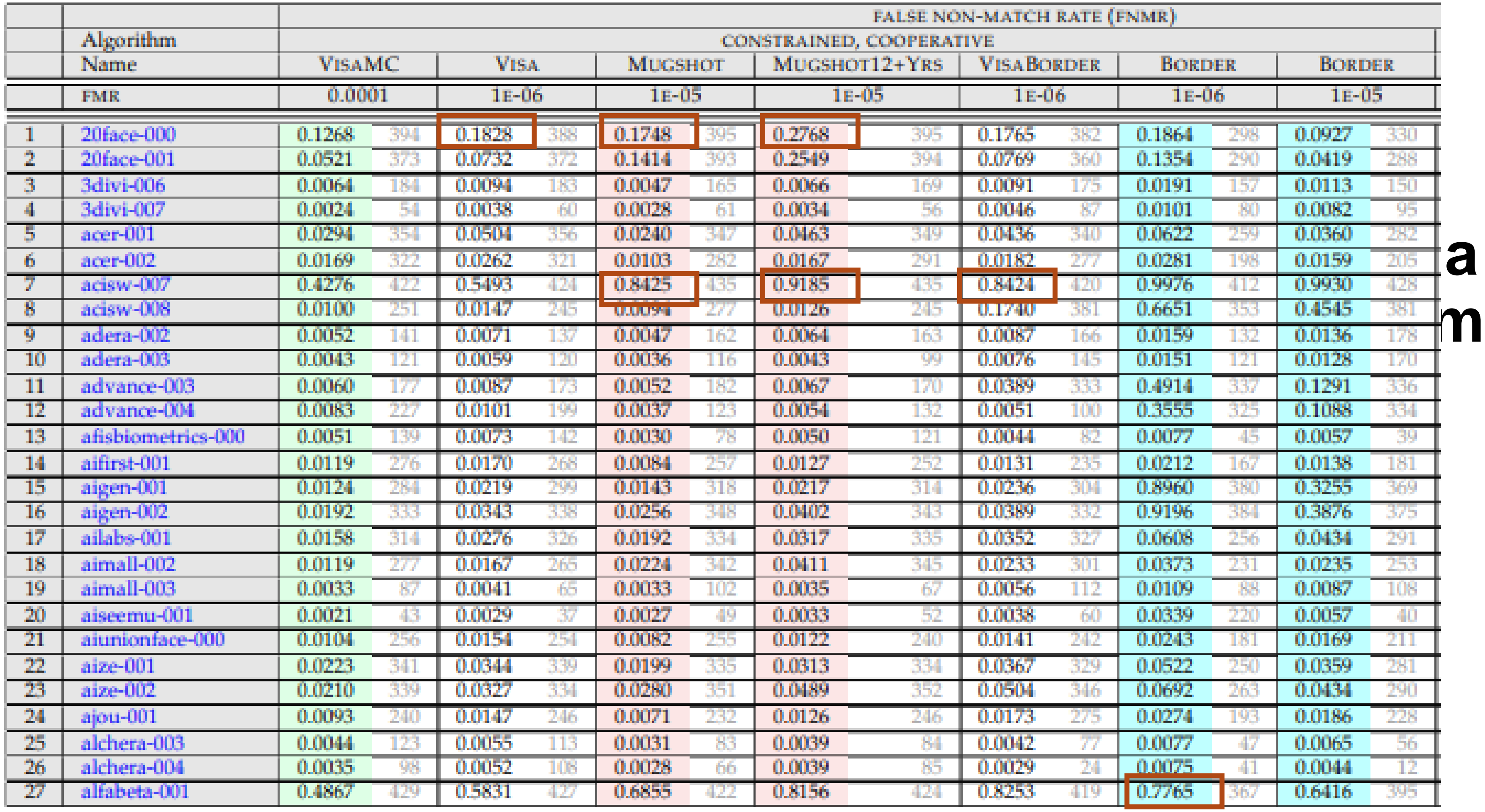
<u>Proble</u>

Accura

- **A “fa a biom me perso**

https://www.nist.gov/progr

N



	Algorithm Name	FALSE NON-MATCH RATE (FNMR) CONSTRAINED, COOPERATIVE VISAMC		VISA		MUGSHOT		MUGSHOT12+YRS		VISABORDER		BORDER		BORDER	
	FMR	0.0001		1E-06		1E-05		1E-05		1E-06		1E-06		1E-05	
1	20face-000	0.1268	394	0.1828	388	0.1748	395	0.2768	395	0.1765	382	0.1864	298	0.0927	330
2	20face-001	0.0521	373	0.0732	372	0.1414	393	0.2549	394	0.0769	360	0.1354	290	0.0419	288
3	3divi-006	0.0064	184	0.0094	183	0.0047	165	0.0066	169	0.0091	175	0.0191	157	0.0113	150
4	3divi-007	0.0024	54	0.0038	60	0.0028	61	0.0034	56	0.0046	87	0.0101	80	0.0082	95
5	acer-001	0.0294	354	0.0504	356	0.0240	347	0.0463	349	0.0436	340	0.0622	259	0.0360	282
6	acer-002	0.0169	322	0.0262	321	0.0103	282	0.0167	291	0.0182	277	0.0281	198	0.0159	205
7	acisw-007	0.4276	422	0.5493	424	0.8425	435	0.9185	435	0.8424	420	0.9976	412	0.9930	428
8	acisw-008	0.0100	251	0.0147	245	0.0094	277	0.0126	245	0.1740	381	0.6651	353	0.4545	381
9	adera-002	0.0052	141	0.0071	137	0.0047	162	0.0064	163	0.0087	166	0.0159	132	0.0136	178
10	adera-003	0.0043	121	0.0059	120	0.0036	116	0.0043	99	0.0076	145	0.0151	121	0.0128	170
11	advance-003	0.0060	177	0.0087	173	0.0052	182	0.0067	170	0.0389	333	0.4914	337	0.1291	336
12	advance-004	0.0083	227	0.0101	199	0.0037	123	0.0054	132	0.0051	100	0.3555	325	0.1088	334
13	afisbiometrics-000	0.0051	139	0.0073	142	0.0030	78	0.0050	121	0.0044	82	0.0077	45	0.0057	39
14	aifirst-001	0.0119	276	0.0170	268	0.0084	257	0.0127	252	0.0131	235	0.0212	167	0.0138	181
15	aigen-001	0.0124	284	0.0219	299	0.0143	318	0.0217	314	0.0236	304	0.8960	380	0.3255	369
16	aigen-002	0.0192	333	0.0343	338	0.0256	348	0.0402	343	0.0389	332	0.9196	384	0.3876	375
17	ailabs-001	0.0158	314	0.0276	326	0.0192	334	0.0317	335	0.0352	327	0.0608	256	0.0434	291
18	aimall-002	0.0119	277	0.0167	265	0.0224	342	0.0411	345	0.0233	301	0.0373	231	0.0235	253
19	aimall-003	0.0033	87	0.0041	65	0.0033	102	0.0035	67	0.0056	112	0.0109	88	0.0087	108
20	aiseemu-001	0.0021	43	0.0029	37	0.0027	49	0.0033	52	0.0038	60	0.0339	220	0.0057	40
21	aiunionface-000	0.0104	256	0.0154	254	0.0082	255	0.0122	240	0.0141	242	0.0243	181	0.0169	211
22	aize-001	0.0223	341	0.0344	339	0.0199	335	0.0313	334	0.0367	329	0.0522	250	0.0359	281
23	aize-002	0.0210	339	0.0327	334	0.0280	351	0.0489	352	0.0504	346	0.0692	263	0.0434	290
24	ajou-001	0.0093	240	0.0147	246	0.0071	232	0.0126	246	0.0173	275	0.0274	193	0.0186	228
25	alchera-003	0.0044	123	0.0055	113	0.0031	83	0.0039	84	0.0042	77	0.0077	47	0.0065	56
26	alchera-004	0.0035	98	0.0052	108	0.0028	66	0.0039	85	0.0029	24	0.0075	41	0.0044	12
27	alfabeta-001	0.4867	429	0.5831	427	0.6855	422	0.8156	424	0.8253	419	0.7765	367	0.6416	395

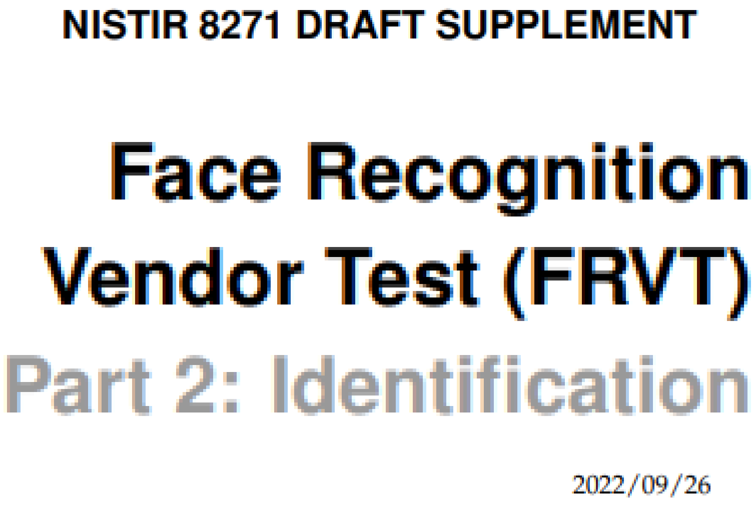
NIST wants false match rate = 0.00001 as a goal or 1:100,000 errors

KnowBe4
Human error. Conquered.

Biometric Basics

Problems

Accuracy



NISTIR 8271 DRAFT SUPPLEMENT

Face Recognition Vendor Test (FRVT)

Part 2: Identification

2022/09/26

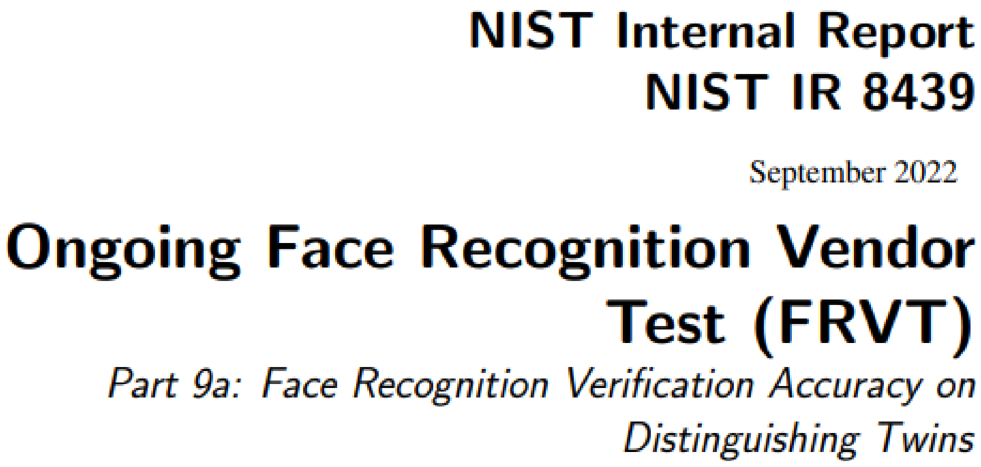
"Recognition accuracy is very strongly dependent on the algorithm and, more generally, on the developer of the algorithm. False negative error rates in a particular scenario range from a few tenths of one percent to beyond fifty percent."

https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

Biometric Basics

Problems

Accuracy - Twins



NIST Internal Report
NIST IR 8439

September 2022

Ongoing Face Recognition Vendor Test (FRVT)

Part 9a: Face Recognition Verification Accuracy on Distinguishing Twins

“All of the algorithms submitted to the FRVT verification track are unable to distinguish between identical twins.”

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8439.pdf

Biometric Basics

Accuracy –Example: Voice-Recognition

1. Attacker captures victim’s voice

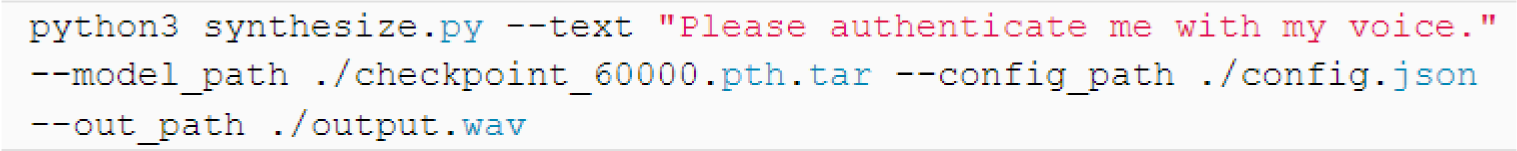
    Multiple times is better

2. Uses deepfake technology to create new phrases
3. Uses against people or voice-recognition technology

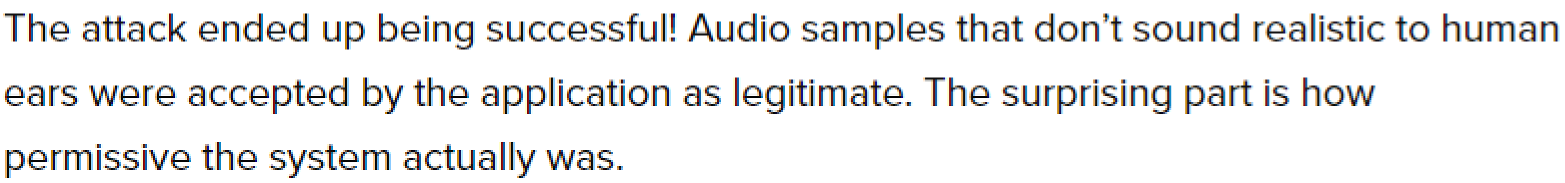
Biometric Basics

Accuracy –Example: Voice-Recognition

- Red team tried to get past Help Desk voice recognition system used to authenticate people calling into Help Desk



```
python3 synthesize.py --text "Please authenticate me with my voice."
--model_path ./checkpoint_60000.pth.tar --config_path ./config.json
--out_path ./output.wav
```



The attack ended up being successful! Audio samples that don't sound realistic to human ears were accepted by the application as legitimate. The surprising part is how permissive the system actually was.

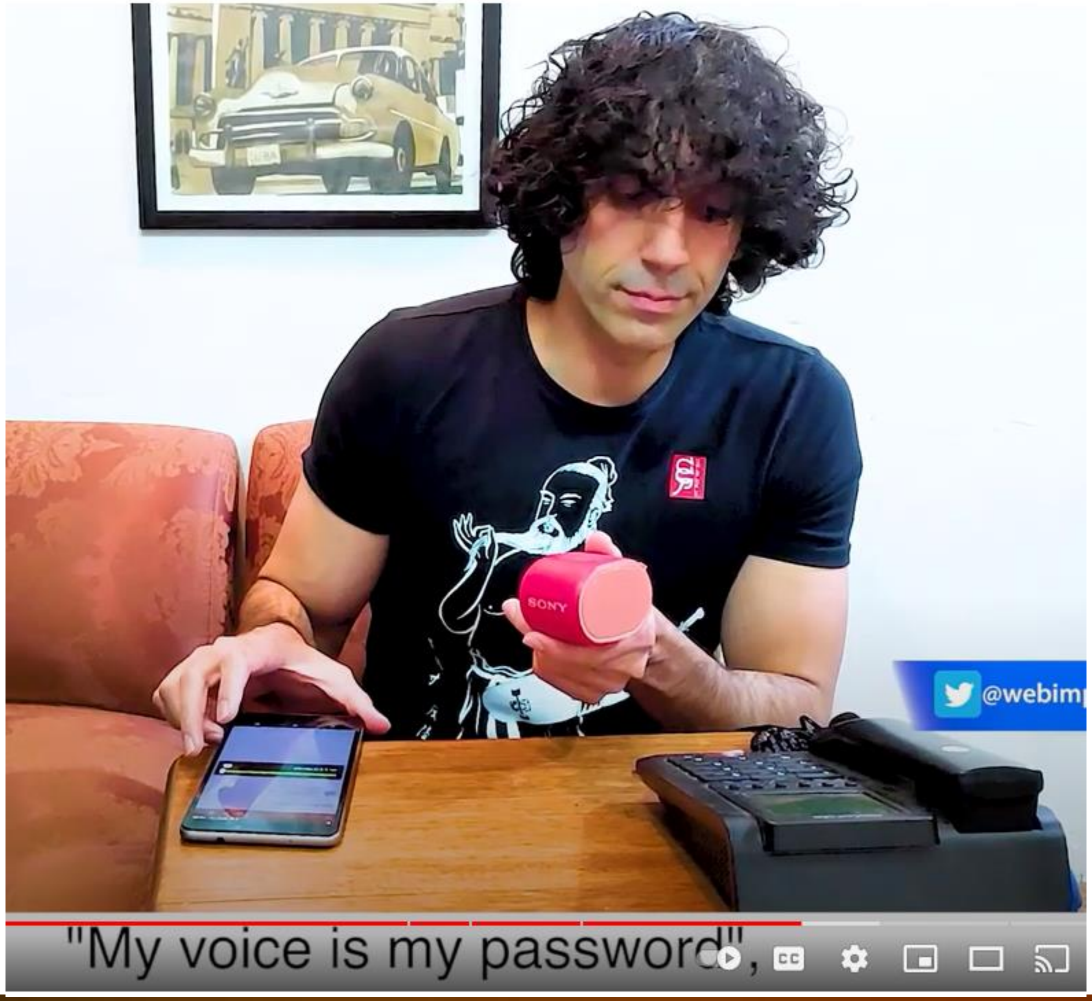
https://www.netspi.com/blog/technical/adversary-simulation/using-deep-fakes-to-bypass-voice-biometrics/

Biometric Basics

Accuracy –Example: Voice-Recognition

- Cybersecurity expert fools bank’s voice recognition system

https://www.youtube.com/watch?v=CeYLyeWhi4E



Biometric Basics

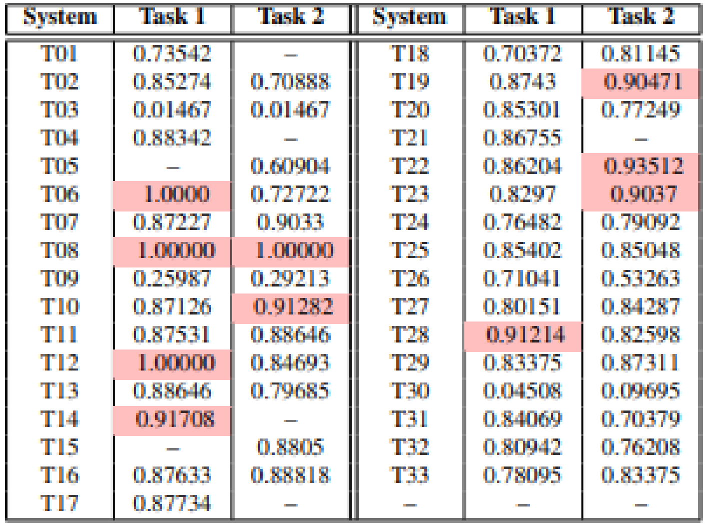
Accuracy –Example: Voice-Recognition

Voice Conversion Challenge 2020

http://www.vc-challenge.org/

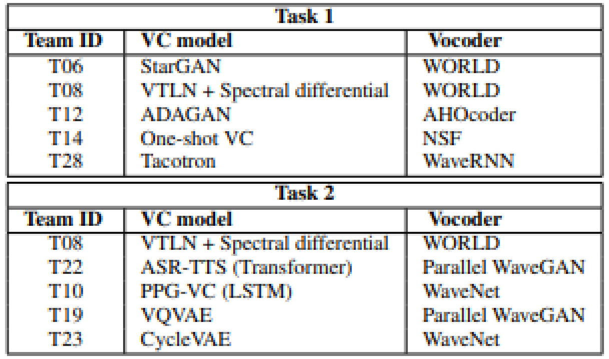
1.0000=100% Detection of Deepfake Spoof,
Higher is better

Table 7: *Minimum t-DCF for each system of VCC 2020. Red cells indicate top-5 systems for each task.*



System	Task 1	Task 2	System	Task 1	Task 2
T01	0.73542	–	T18	0.70372	0.81145
T02	0.85274	0.70888	T19	0.8743	0.90471
T03	0.01467	0.01467	T20	0.85301	0.77249
T04	0.88342	–	T21	0.86755	–
T05	–	0.60904	T22	0.86204	0.93512
T06	1.0000	0.72722	T23	0.8297	0.9037
T07	0.87227	0.9033	T24	0.76482	0.79092
T08	1.00000	1.00000	T25	0.85402	0.85048
T09	0.25987	0.29213	T26	0.71041	0.53263
T10	0.87126	0.91282	T27	0.80151	0.84287
T11	0.87531	0.88646	T28	0.91214	0.82598
T12	1.00000	0.84693	T29	0.83375	0.87311
T13	0.88646	0.79685	T30	0.04508	0.09695
T14	0.91708	–	T31	0.84069	0.70379
T15	–	0.8805	T32	0.80942	0.76208
T16	0.87633	0.88818	T33	0.78095	0.83375
T17	0.87734	–	–	–	–

Table 8: *Details of top-performing VC systems in terms of minimum t-DCF as a spoofing threat.*



Task 1		
Team ID	**VC model**	**Vocoder**
T06	StarGAN	WORLD
T08	VTLN + Spectral differential	WORLD
T12	ADAGAN	AHOcoder
T14	One-shot VC	NSF
T28	Tacotron	WaveRNN
Task 2		
Team ID	**VC model**	**Vocoder**
T08	VTLN + Spectral differential	WORLD
T22	ASR-TTS (Transformer)	Parallel WaveGAN
T10	PPG-VC (LSTM)	WaveNet
T19	VQVAE	Parallel WaveGAN
T23	CycleVAE	WaveNet

> “The VCC evaluation report indicates the merits of voice conversion are improving drastically in different aspects like naturalness, speaker similarity, amount of target voice needed to create a deepfake and robustness in synthesizing in real time.”
>
> Forbes, May 2021

Biometric Basics

Bias

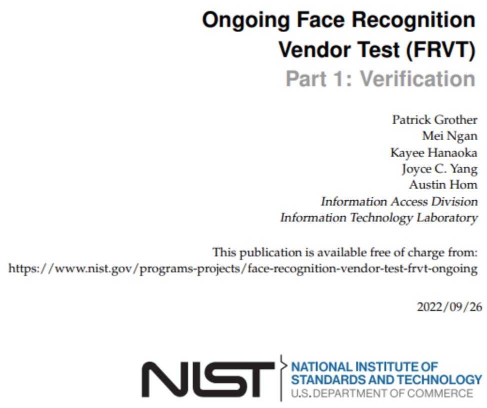
- Biometric solutions can have **TECHNICAL** higher false-positive and false-negative rates with particular populations
- “Performance variability due to demographics”
  - -Dr. Stephanie Schuckers, Director of CITeR, Clarkson University
- Often due to skin color
- Not talking about someone’s personal bias

Biometric Basics

Problems

Bias

- **A “false non-match rate” or FNMR is the rate at which a biometric solution says the same person is not the same person**



Ongoing Face Recognition Vendor Test (FRVT)

Part 1: Verification

Patrick Grother
Mei Ngan
Kayee Hanaoka
Joyce C. Yang
Austin Hom
Information Access Division
Information Technology Laboratory

This publication is available free of charge from:
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

2022/09/26

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

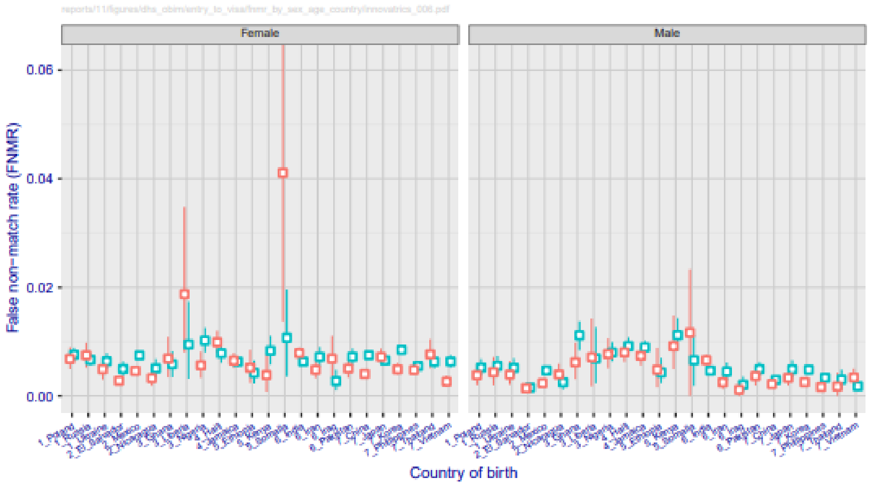
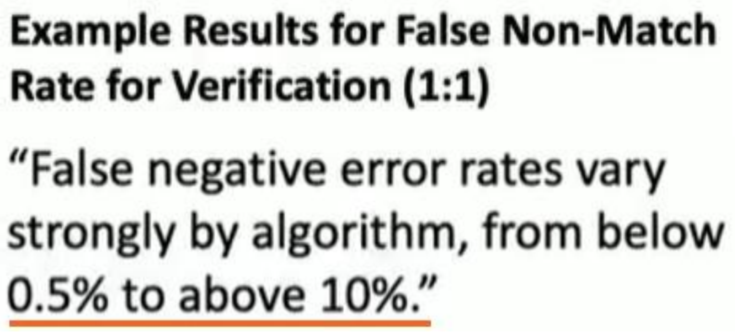


Figure 57: FNMR by sex, age and country of birth, innovatrics-006



Example Results for False Non-Match Rate for Verification (1:1)

“False negative error rates vary strongly by algorithm, from below 0.5% to above 10%.”

https://pages.nist.gov/frvt/reports/demographics/annexes/annex_14.pdf

Biometric Basics

Bias

Can be an economic problem, for example:

- Poorer people might be less likely to be able to afford a cell phone capable of doing fingerprints
- Might have more fingerprint abrasions due to hard work
- May have less experience with using a smartphone
- May not have a smartphone or any cell phone
  - 25% of the world does not have a cell phone
- May share a phone with someone else
  - May not even trust that person

Biometric Basics

Bias

Can be a disability problem, for example:

- Sight impaired
- Uncontrolled tremors
- Missing biometric trait being measured

Biometric Basics

Summary Lesson

Some biometric solutions are more accurate than others

You need to know which you are buying/using

Agenda

- Biometric Basics
- Hacking Biometrics
- Safer Biometrics

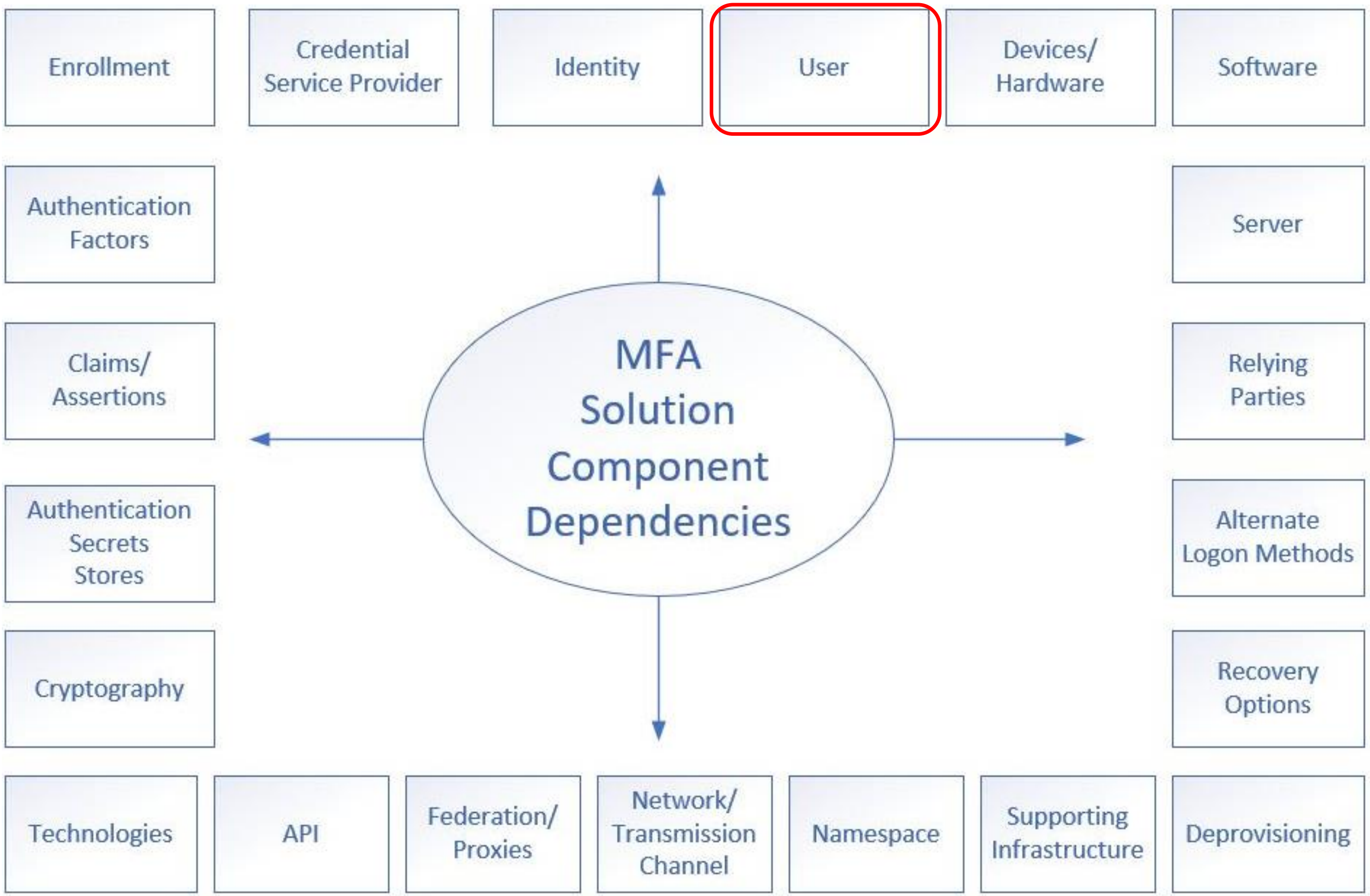
Hacking Biometrics

Summary

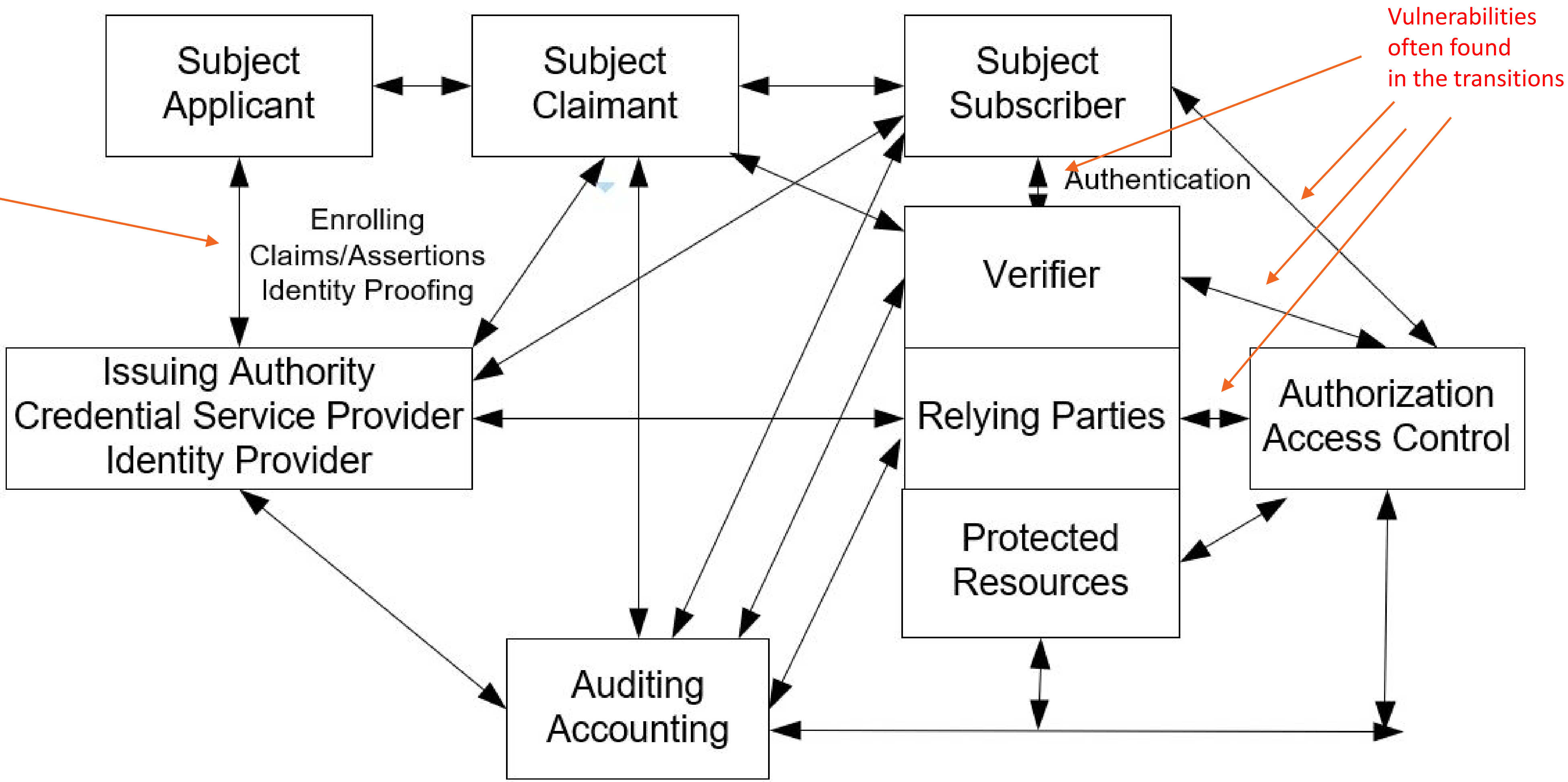
Hack the:

- Biometric Reader and/or process
- Any other component involved
- MitM/AitM Attacks
- Fake the biometric attribute (i.e., Presentation Attacks)
- Steal attributes

Hacking Biometrics



Hacking Biometrics



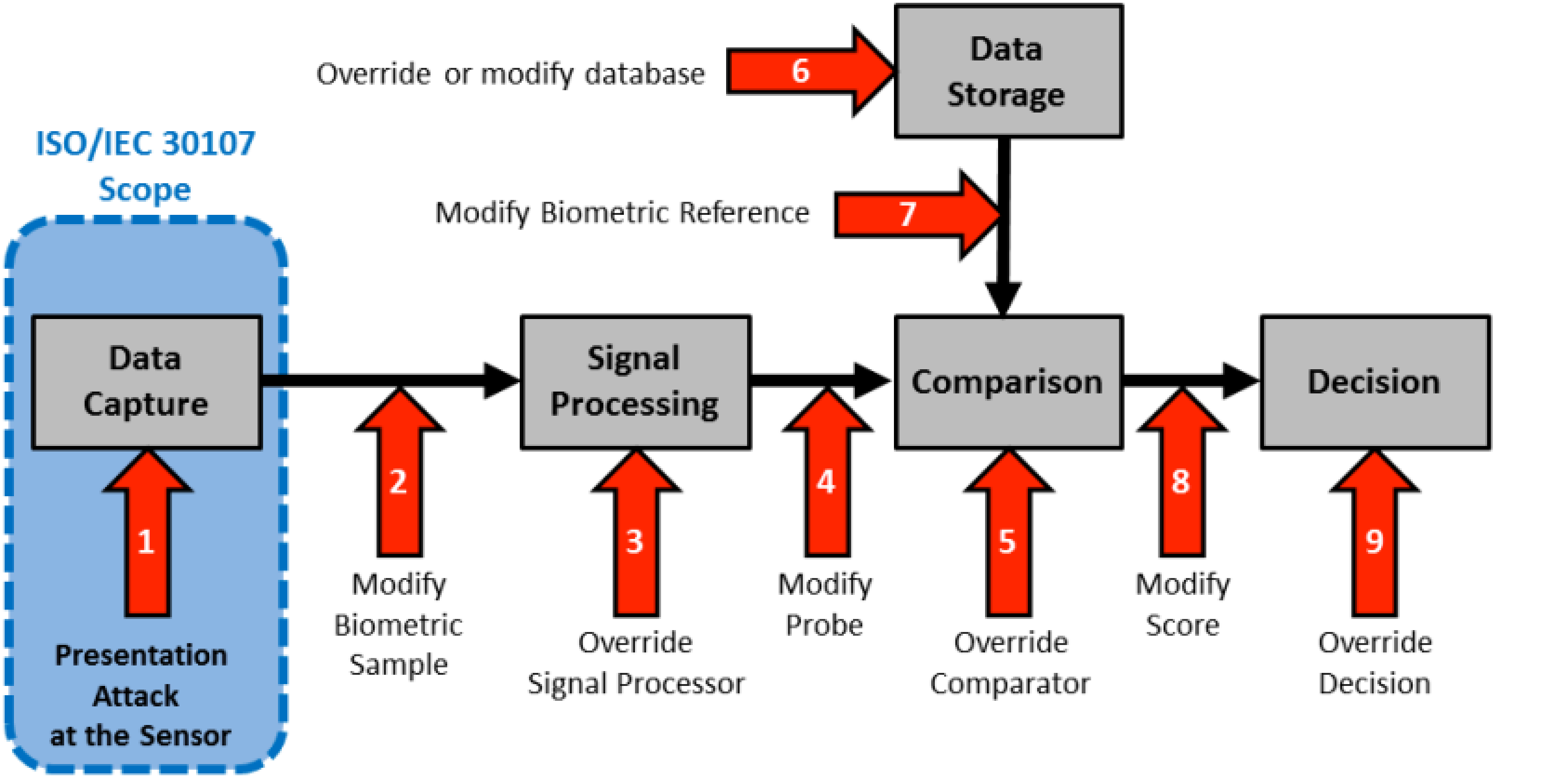
Vulnerabilities often found in the transitions

Vulnerabilities often found in the transitions

KnowBe4
Human error. Conquered.

Hacking Biometrics

Hacks on Biometric Device/Reader/ System Itself



Source: ISO/IEC 30107-1
Inspired by N.K. Ratha, J.H. Connell, R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, Vol 40. NO 3, 2001.

From: https://www.nist.gov/system/files/documents/2020/09/15/12_buschthieme-ibpc-pad-160504.pdf

Hacking Biometrics

Hacking Methodology

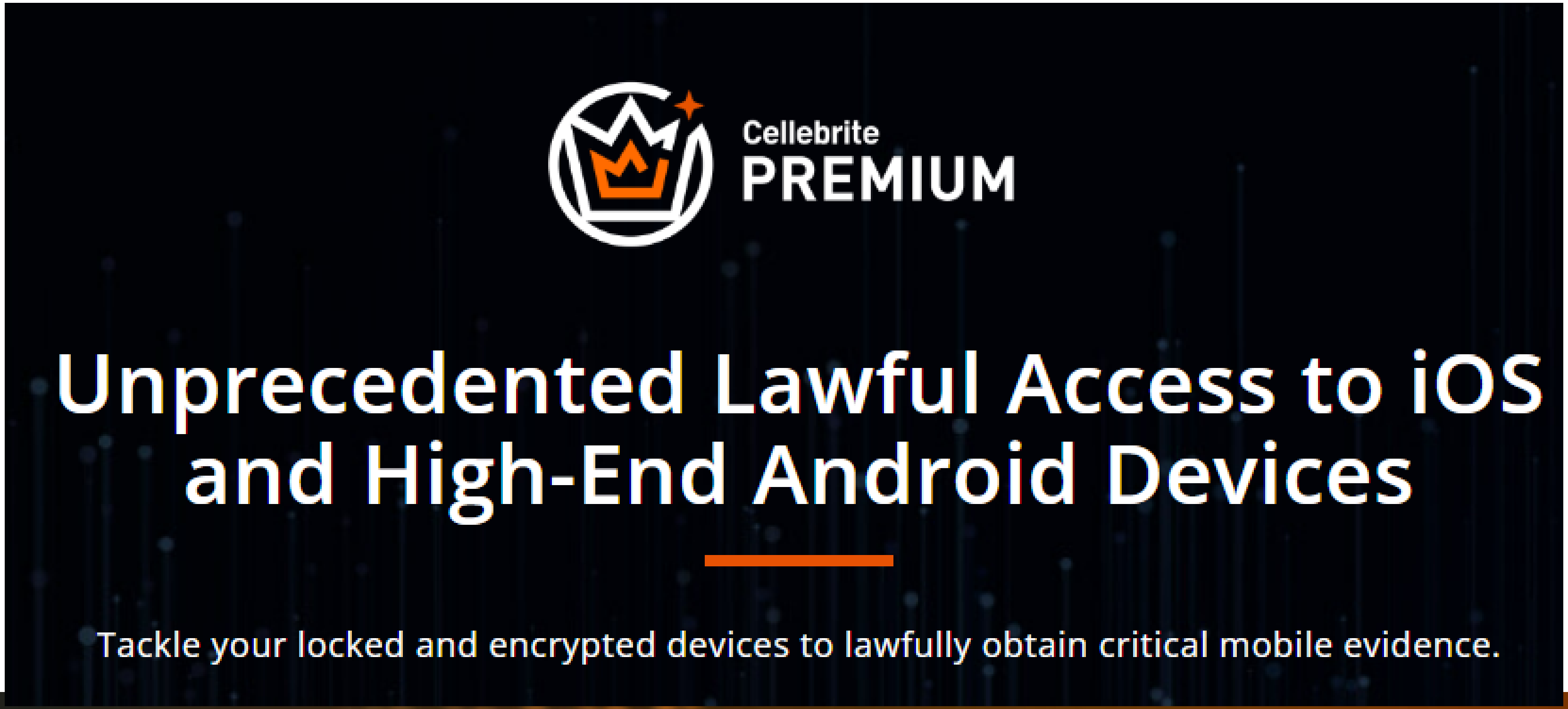
Basic attack methods that work against most biometric solutions

- Social Engineering (most popular and successful method)
- Eavesdropping/MitM
- Exploit Programming bug
- Weak verification between components
- Alternate recovery/bypass
- Weak default configuration settings
- Data/Network traffic malformation
- 3rd Party Reliance issue (e.g., DNS, Active Directory, etc.)
- Physical attacks
- Others

Hacking Biometrics

Bypass Attacks

There are dozens to hundreds of companies with products that bypass phone lock screens



Cellebrite PREMIUM

Unprecedented Lawful Access to iOS and High-End Android Devices

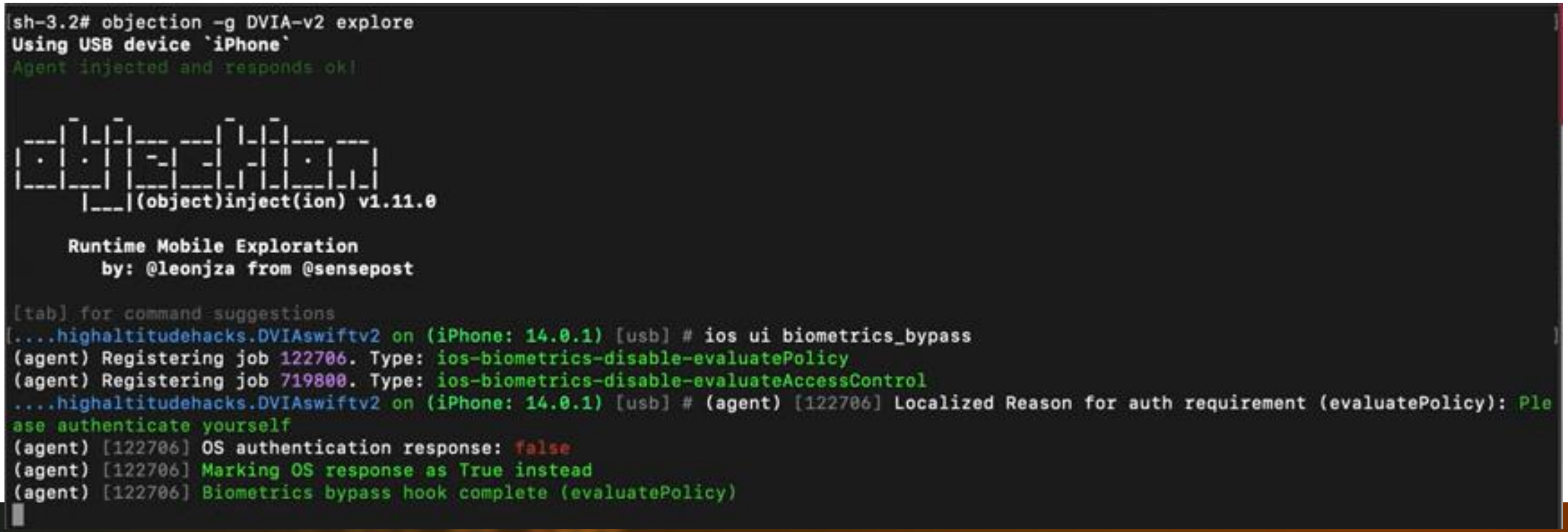
Tackle your locked and encrypted devices to lawfully obtain critical mobile evidence.

Hacking Biometrics

Bypass Attacks

There are often bugs which allows a knowledgeable attacker to bypass the biometric screening

- Run exploit code in debug session: https://www.youtube.com/watch?v=QHY_gtCM7y0



```
sh-3.2# objection -g DVIA-v2 explore
Using USB device `iPhone`
Agent injected and responds ok!

     _   _         _   _
 ___| |_|_|___ ___| |_|_|___ ___
| . | . | | -_|  _|  _| | . |   |
|___|___| |___|___|_| |_|___|_|_|
      |___|(object)inject(ion) v1.11.0

     Runtime Mobile Exploration
        by: @leonjza from @sensepost

[tab] for command suggestions
....highaltitudehacks.DVIAswiftv2 on (iPhone: 14.0.1) [usb] # ios ui biometrics_bypass
(agent) Registering job 122706. Type: ios-biometrics-disable-evaluatePolicy
(agent) Registering job 719800. Type: ios-biometrics-disable-evaluateAccessControl
....highaltitudehacks.DVIAswiftv2 on (iPhone: 14.0.1) [usb] # (agent) [122706] Localized Reason for auth requirement (evaluatePolicy): Ple
ase authenticate yourself
(agent) [122706] OS authentication response: false
(agent) [122706] Marking OS response as True instead
(agent) [122706] Biometrics bypass hook complete (evaluatePolicy)
```

KnowBe4
Human error. Conquered.

Hacking Biometrics

<u>Bypass Attacks</u>

There are often bugs which allows a knowledgeable attacker to bypass the biometric screening

- Trick app into bypassing biometric lock screen, and use it to access device
- On phone: Use emergency phone number screen to cause a phone reset: https://www.youtube.com/watch?v=TnKChcnX0KQ

Hacking Biometrics

Presentation Attacks

Presentation Attack = submitting fraudulently created biometric attribute

- ISO/IEC 30107-3:2017

  https://www.iso.org/standard/67381.html

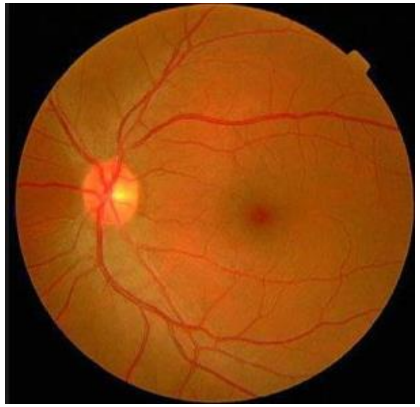
  - Deals with automated detection of presentation attacks (i.e., Presentation Attack Detection (PAD)

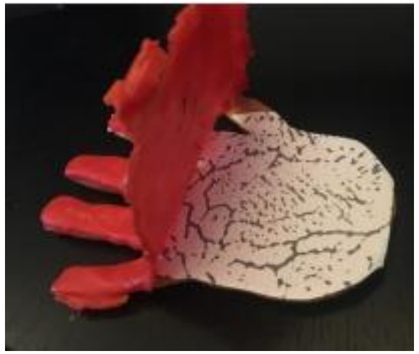
Biometric Fakes

PAD Attacks

Biometric Recreations

- Fake fingerprints, fake faces, deepfake voices, etc.
    - Biometric vendors try to prevent fakes, but hackers just get around
- Stolen and replayed



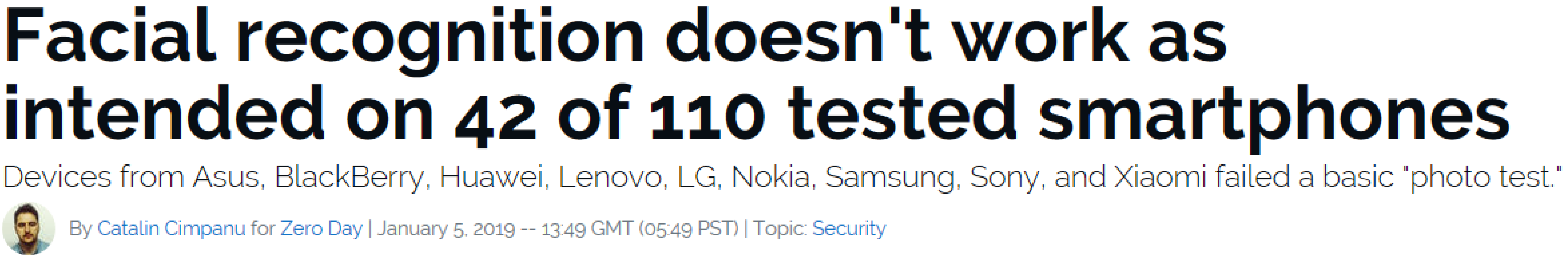


MFA Hacks

Physical Attacks

Biometric – Fake Faces

- Pictures
- 3D Masks
- Photoshopped blinking eyelids in animated gifs



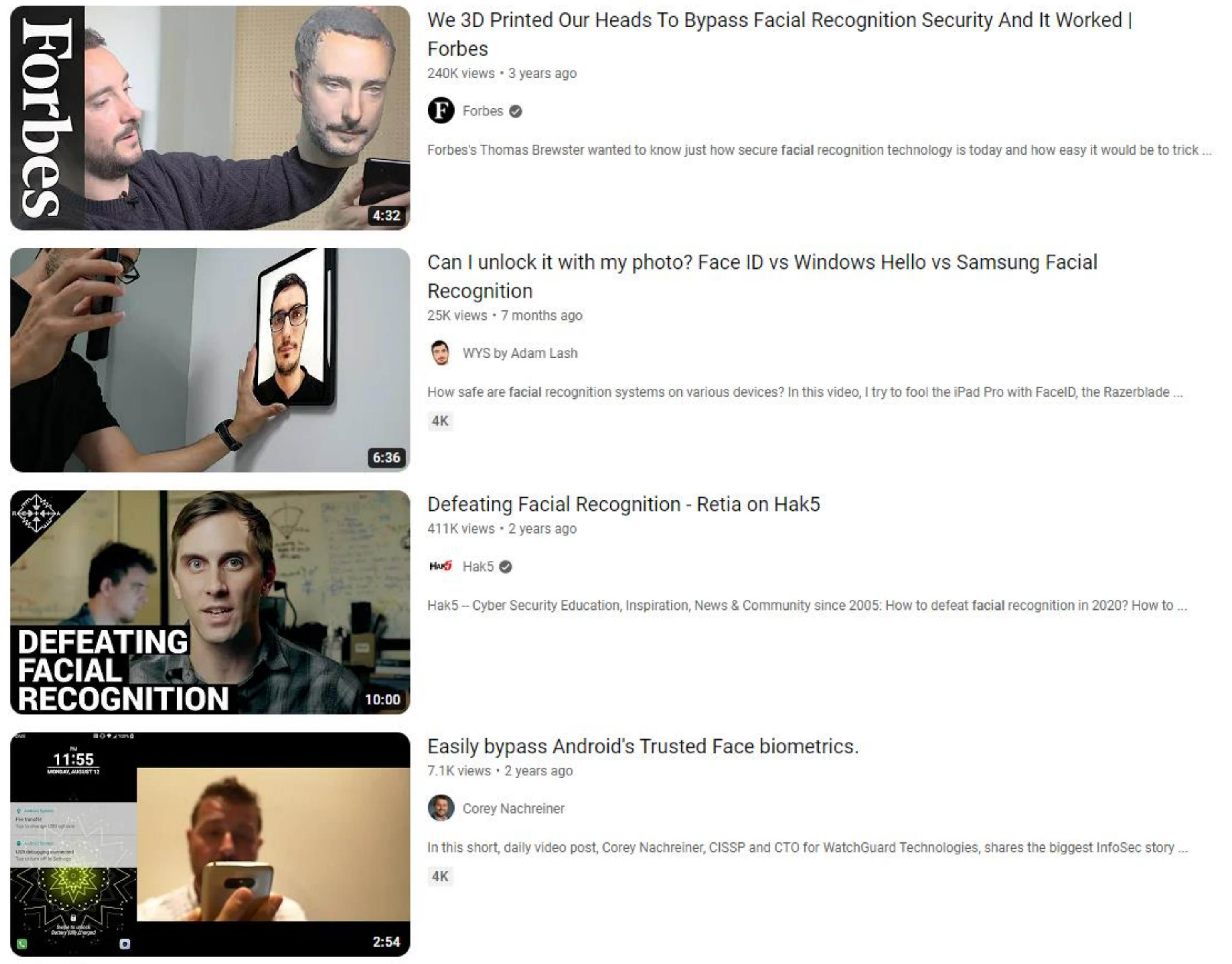
Facial recognition doesn't work as intended on 42 of 110 tested smartphones

Devices from Asus, BlackBerry, Huawei, Lenovo, LG, Nokia, Samsung, Sony, and Xiaomi failed a basic "photo test."

By Catalin Cimpanu for Zero Day | January 5, 2019 -- 13:49 GMT (05:49 PST) | Topic: Security

MFA Hacks

YouTube Video Search



We 3D Printed Our Heads To Bypass Facial Recognition Security And It Worked | Forbes

240K views • 3 years ago

Forbes

Forbes's Thomas Brewster wanted to know just how secure **facial** recognition technology is today and how easy it would be to trick ...

Can I unlock it with my photo? Face ID vs Windows Hello vs Samsung Facial Recognition

25K views • 7 months ago

WYS by Adam Lash

How safe are **facial** recognition systems on various devices? In this video, I try to fool the iPad Pro with FaceID, the Razerblade ...

4K

Defeating Facial Recognition - Retia on Hak5

411K views • 2 years ago

Hak5

Hak5 -- Cyber Security Education, Inspiration, News & Community since 2005: How to defeat **facial** recognition in 2020? How to ...

Easily bypass Android's Trusted Face biometrics.

7.1K views • 2 years ago

Corey Nachreiner

In this short, daily video post, Corey Nachreiner, CISSP and CTO for WatchGuard Technologies, shares the biggest InfoSec story ...

4K

Safer Biometrics

Liveness Detection

Is the attribute being presented to the biometric reader involve a live person?

- Look for changing light, heat, 3D geometry bouncing off face
- Look for blinking eyes
- Look for blood flow

Safer Biometrics

Liveness Detection

- Hackers and researchers always trying to fool liveness detection
- Often successful
- Face - Using 3D masks, silicon masks, video of person

LivDet Liveness Detection Competition Series

http://livdet.org/

Safer Biometrics

Liveness Detection

Face Liveness Detection Competition (LivDet-Face) - 2021

https://livdet.org/face2021-livdet-org/face_2021.pdf

- The winning solution of the image category convinced facial scanners to accept fake images 16.47% of the time

Safer Biometrics

Liveness Detection

Apple FaceID

- Didn’t fail amateur silicon mask trick
- https://www.youtube.com/watch?v=FhbMLmsCax0

Safer Biometrics

Liveness Detection

Make sure what you're using is one of the accurate solutions

- Look for ISO/IEC 30107-3
- NIST PAD testing standard coming soon
- NIST NVLAP accrediting independent labs, like
- iBeta independent lab

Safer Biometrics

Continuous Detection

- Instead of measuring once, measure all the time?
- Part of zero-trust initiative
- Layer traditional logon security partnered with keystroke/cursor dynamics?

Man-in-the-Middle Attacks

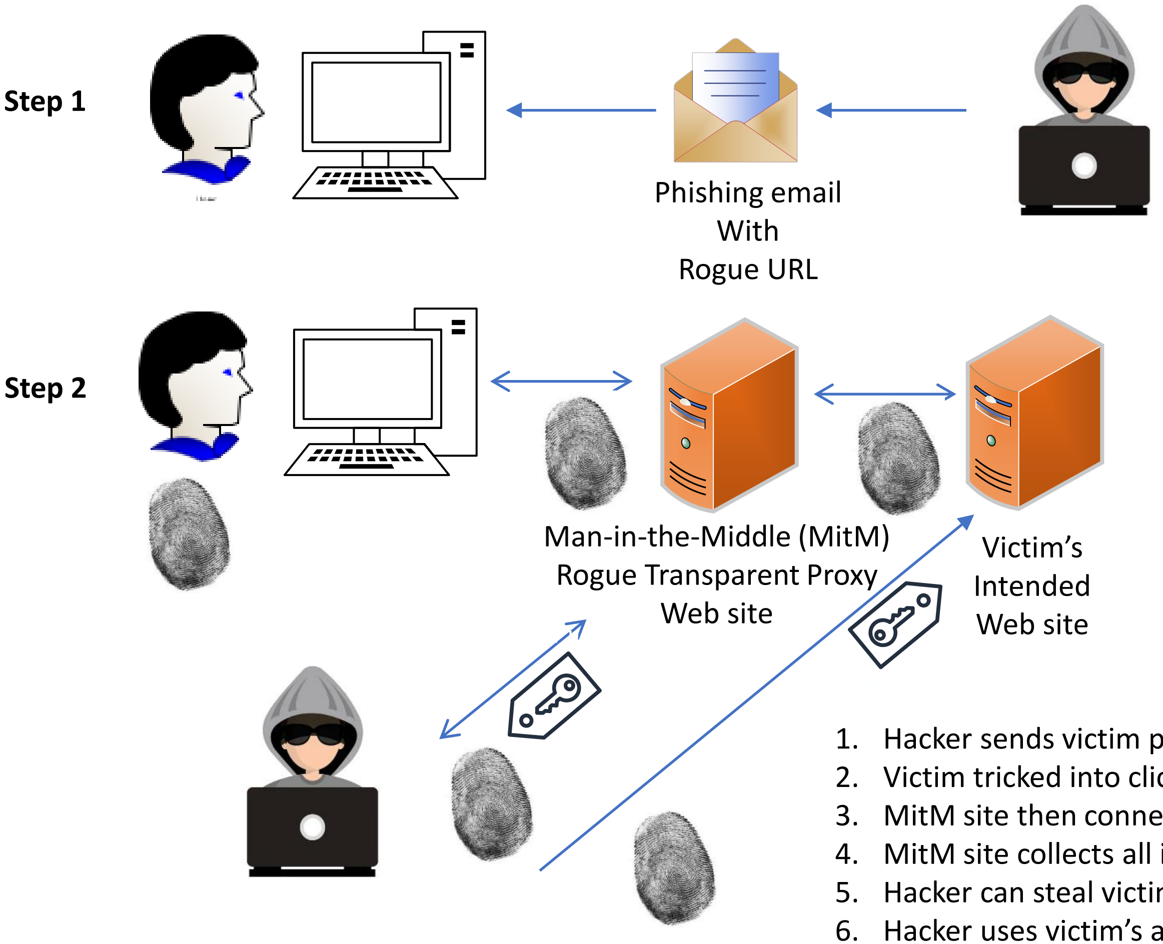
Copied Biometrics

- There is nothing inherent in biometrics that stops Man-in-the-Middle (MitM) attacks
- If an attacker can insert themselves between client and the server and neither side is able to tell, then the method is susceptible to MitM attacks

MFA Bypass Hack

Network Session Hijacking

Network Session Hijacking Proxy Theft Logical Diagram

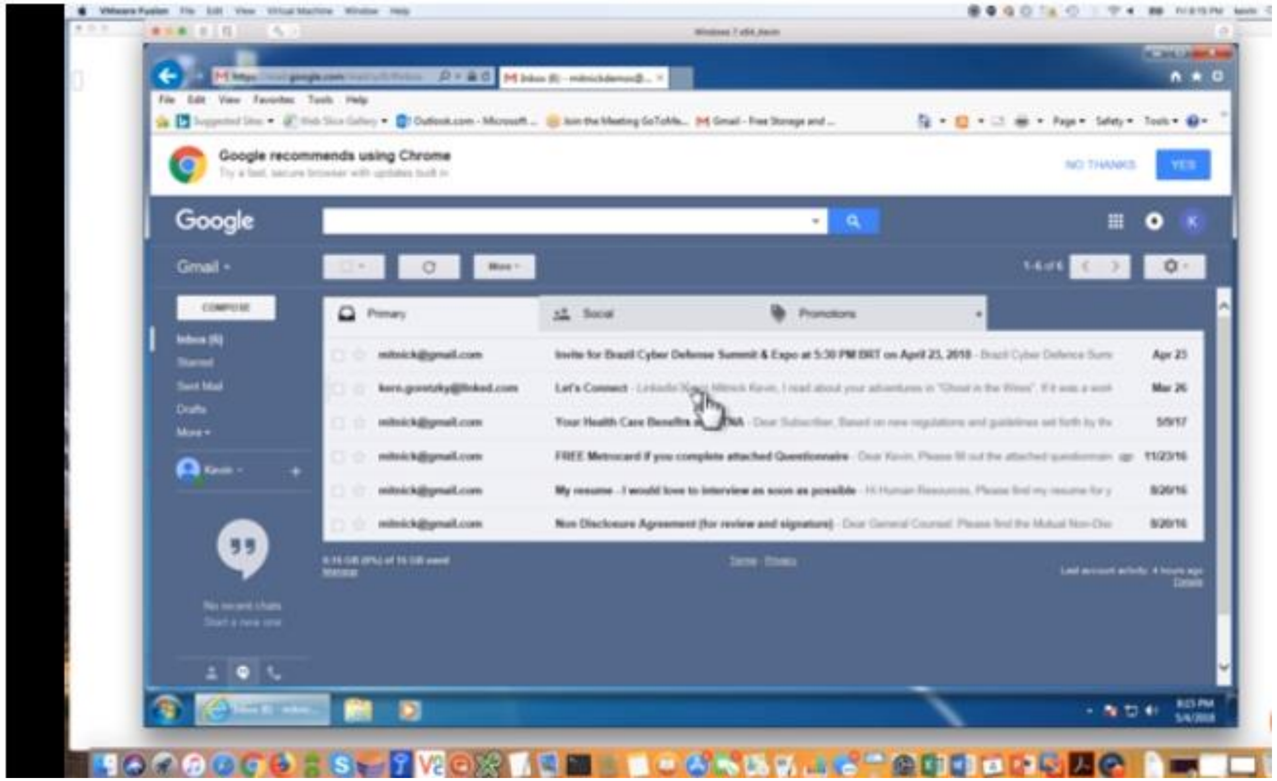


1. Hacker sends victim phishing email with rogue URL
2. Victim tricked into clicking on rogue URL, taking victim to rogue MitM site
3. MitM site then connects to victim's intended legitimate, real, web site
4. MitM site collects all info/data sent between victim and real web site; and vice-versa
5. Hacker can steal victim's logon creds, bio attrib, access control token cookie, etc.
6. Hacker uses victim's access control token cookie to logon

MFA Hacks

Network Session Hijacking

Kevin Mitnick Hack Demo



mitnick@gmail.com	Invite for Brazil Cyber Defense Summit & Expo at 5:30 PM BRT on April 23, 2018 - Brazil Cyber Defence Sum	Apr 23
kera.goretzky@linked.com	Let's Connect - LinkedIn Kevin Mitnick Kevin, I read about your adventures in "Ghost in the Wires". If it was a work	Mar 26
mitnick@gmail.com	Your Health Care Benefits a... NA - Dear Subscriber, Based on new regulations and guidelines set forth by the	5/9/17
mitnick@gmail.com	FREE Metrocard if you complete attached Questionnaire - Dear Kevin, Please fill out the attached questionnaire	11/23/16
mitnick@gmail.com	My resume - I would love to interview as soon as possible - Hi Human Resources, Please find my resume for y	8/20/16
mitnick@gmail.com	Non Disclosure Agreement (for review and signature) - Dear General Counsel, Please find the Mutual Non-Dis	8/20/16

https://blog.knowbe4.com/heads-up-new-exploit-hacks-linkedin-2-factor-auth.-see-this-kevin-mitnick-video

Man-in-the-Middle Attacks

Copied Biometrics

- Although most biometrics are involved in device logons and not app logons, making them less likely to be MitM'd
- But this does not mean fully resistant
- Remote biometric logons are becoming far more common
- Is biometric auth?:
  - On local device (most common, less susceptible)
  - Or remotely (less common, growing, more susceptible)
- Good if biometric solution cannot be MitM'd either way

Stolen Biometric Attributes

Reuse Stolen Biometrics

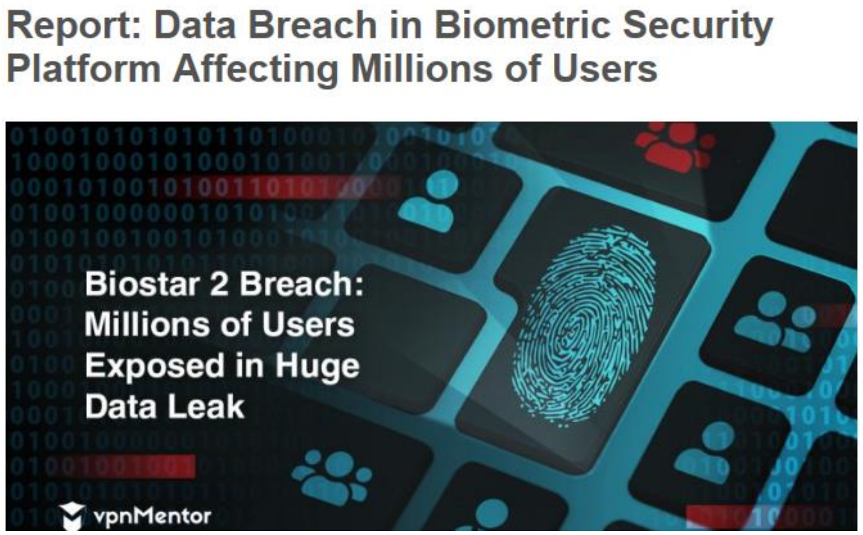
- If your biometric identity is stolen, how do you stop a bad guy from re-using it?
- Once stolen, it’s compromised for your life
- You can change a password or smartcard, you can’t easily change your retina veins or fingerprint
- Known as non-repudiation attack in the crypto world

Example: June 2015 OPM attack stole biometrics of 5.6 million people

https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach

Stolen Biometric Attributes

Reuse Stolen Biometrics



Report: Data Breach in Biometric Security Platform Affecting Millions of Users

Biostar 2 Breach: Millions of Users Exposed in Huge Data Leak
vpnMentor

Another example:

- Aug. 2019 breach
- Biostar2 platform
- Fingerprints and facial recog
- Top 50 biometric app vendor
- Over 1 million fingerprints breached
- The breachers claim company was largely unresponsive and uncooperative to their reports and ongoing discussions

Agenda

- Biometric Basics
- Hacking Biometrics
- Safer Biometrics

Safer Biometrics

<u>Summary</u>

- Choose an Accurate solution
- Choose a Secure solution

Choose solutions that:

- Protect storage of biometric attributes
- Prevent presentation attacks
- Prevent MitM attacks
- Recognize the role bias might play

Safer Biometrics

Accuracy

- Make sure the system is accurate
- Not all biometric systems are equally accurate, you must research if you plan to rely on
- Review error rates and compare to competitors
- Don’t just rely on the vendor’s accuracy attestation
- Ask the vendor what algorithm they use and then look up its accuracy
  - Ex. https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing
- Ask for 2-3 large customers to contact that are using the product

Safer Biometrics

Accuracy

- Maybe consider a different, better, biometric system, with more points of measurement
- Example: Too many false-positive matches with a fingerprint scanner
- Move to fingerprint/finger vein geometry
  - More points to consider
  - Less chance of a false-positive

Safer Biometrics

Accuracy

- Sometimes OK is good enough

Safer Biometrics

MFA is Better

- All other things considered equal, MFA is better than 1FA for security

- Is 1FA biometrics ever right for remote logons?

Safer Biometrics

Secure By Design

- Make sure the entire end-to-end solution is secure
- Vendors developers should know and practice secure development lifecycle (SDL)
  - www.microsoft.com/sdl
  - https://wiki.sei.cmu.edu/confluence/
- Vendor should have in-house code review and penetration testing
- Vendor should hire external pen testers
- Vendor should participate in bug bounties

Safer Biometrics

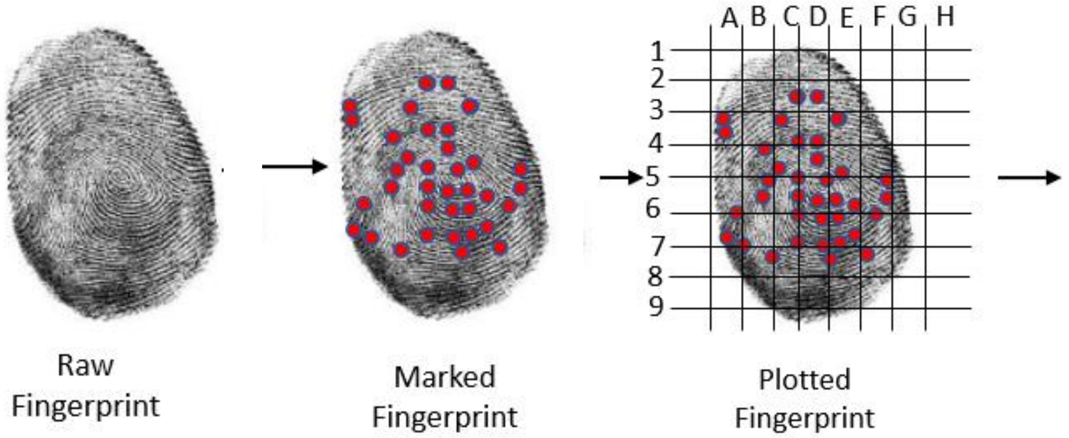
Secure Storage

- How are biometric attributes stored?
  - As exact copies or transformed?
  - You want transformed biometric attribute storage
- Hardware protection is best (TPM chip or something like it)
- Encrypted attributes
- Hashed attributes
- Token attributes

Safer Biometrics

Secure Storage

- Hashed/Token attributes



Raw Fingerprint

Marked Fingerprint

Plotted Fingerprint

C2 A3 A4 C2 D2 E3 E4 B5 C5 D5 E5
A6 B6 D6 E6 D2 F6 G6 A7 B7 C7 D7 E7 F7 F8

Raw Coordinates

957d5703aba3ad26667dd3aa931f3a449e0e0c39d02a5bc9764de7e03c3d72a6
fd126a53827e0aacd1d46c6b1320b4b79647ea585b7868f69a87d481ba7956cf

SHA2-256 Hashed Coordinates

Safer Biometric

Summary

Does biometric solution prevent MitM attacks?

- Is solution susceptible to MitM attacks?
- Would client or server recognize MitM attack?
- FIDO-enabled solutions are resistant to MitM attacks
  - https://fidoalliance.org/certification/biometric-component-certification/

Safer Biometric

<u>Secure</u>

- Submission rate-limiting
- Time-out/lock-out periods for bad submissions

Safer Biometric

Bias

Be Aware of Design and Implementation Biases

- Some solutions have higher biases
- Some populations may not have same awareness, education, capability or availability

Key Takeaways

Parting Thoughts – Education is Necessary

No matter which type of biometrics you choose, educate everyone:

- Buyers, Evaluators, Implementors, Users, Senior management

Topics:

- Strengths and weaknesses
- How to correctly use the biometrics solution
  - Including what might indicate a malicious attempt to abuse it
  - And what to do during rogue attacks
- What biometrics does and doesn’t prevent
- The common possible attacks for that type of biometrics and how to prevent and detect

- You wouldn’t give people passwords without warning them about common hacker tricks

Safer Biometric

More Reading

https://www.biometricsinstitute.org/

https://fidoalliance.org/certification/biometric-component-certification/

https://citer.clarkson.edu/

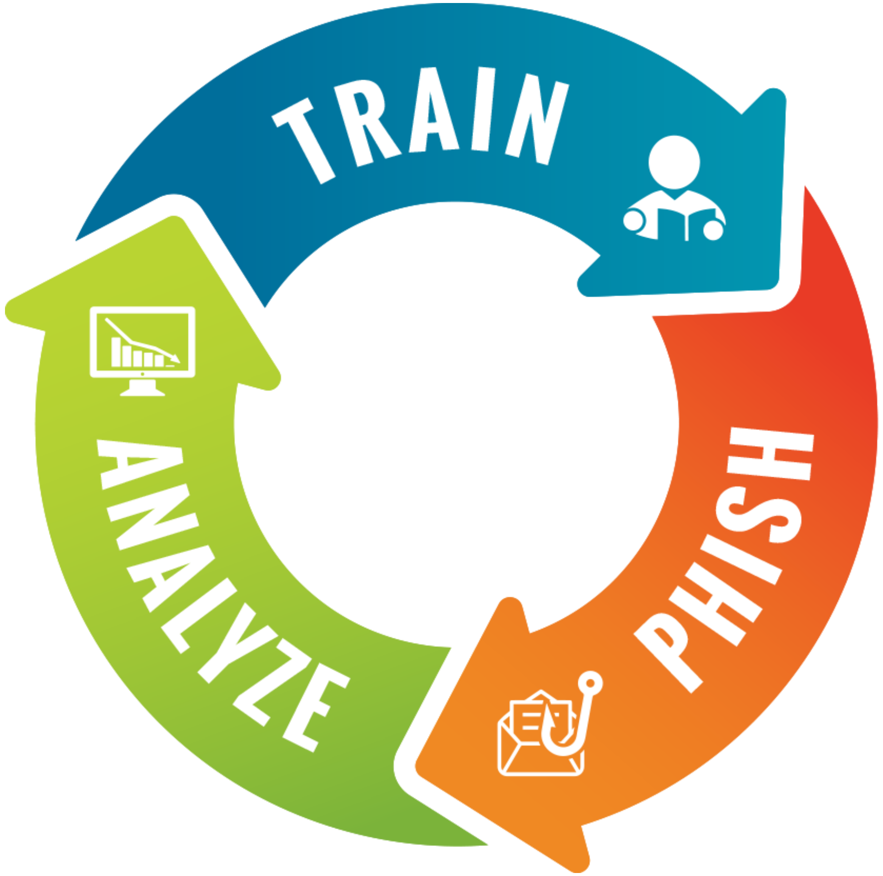
KnowBe4 Security Awareness Training

Baseline Testing
We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

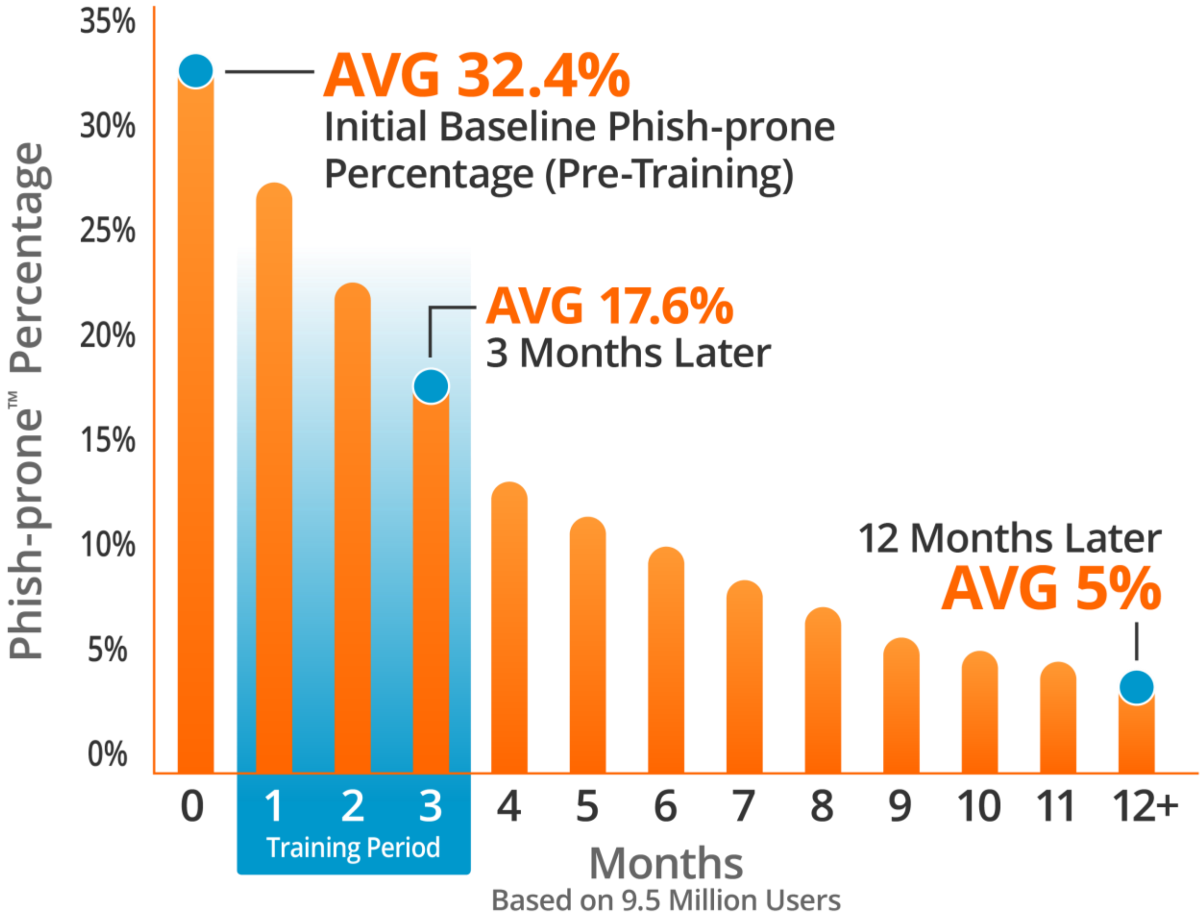


Generating Industry-Leading Results and ROI

- Reduced Malware and Ransomware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

85% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing



Source: 2022 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
https://www.linkedin.com/in/rogeragrimes/