Stopping BOT-enabled cyber attacks through behavioral biometrics.

BSI

WEBINAR SERIES

MFA credentials that kill BOTs.

2023

Stolen, shared and compromised passwords and digital credentials cost corporations billions of dollars in lost revenues each year.

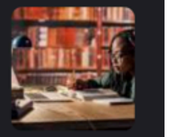
PROBLEM

About 66 results (0.30 seconds)

Forbes

How Higher Education Became The Target Of Bots, Fake Accounts And Online Fraud

As the higher education industry becomes more reliant on technology, it's also becoming more vulnerable to fraud.



ommunity Colleges as

The New York Times

Uber Investigating Breach Computer Systems

The company said on Thursday that it was lo of the apparent hack.

Give this article

A message on Uber's internal system on Thursday told employees, "I announce I am a hacker and Uber has suffered a data breach." Jeff Chiu/Associated Press

Education Beat Podcast — What Albania taught our

EdSource

TOPICS PROJECTS & INVESTIGATIONS

Bot attacks compound enr California Community Coll

College enrollment data across the state no

FOLLOWING COVID MONEY IN EDUCATION

SEPTEMBER 7, 2021

THOMAS PEELE, DANIEL J. WILLIS, LARRY GORDON, AND MICHAEL BURKE

1 COMMENT

The New York Times

f Biden's Forgiveness Program Challenges Reach Supreme Court Income-Driven Repayment Propo

Over 60,000 Fake Applications Submitted in Student Aid Scheme, California Says

It was unclear how much money, if any, was disbursed to the suspicious students. The federal Education Department said it was investigating the suspected fraud.

Give this article

EdSource

Subscribe on iTunes

Listen on Spotify

$Billions in costs and losses

Credential sharing
Identity theft or takeover
Ransomware attacks
eCommerce fraud
Internet robot attacks
Privacy management
Regulatory enforcement

MFA

Multifactor Authentication

IS NOT

…a complete solution.

Conventional passwords and physical biometric factors are regularly:

Shared
Stolen
Replicated
Compromised

PROBLEM

What if we could “plug” the MFA BOT loophole?

What could we do with credentials that can’t be shared, stolen, replicated by any human or machine?

SOLUTION

What is a BOT attack?

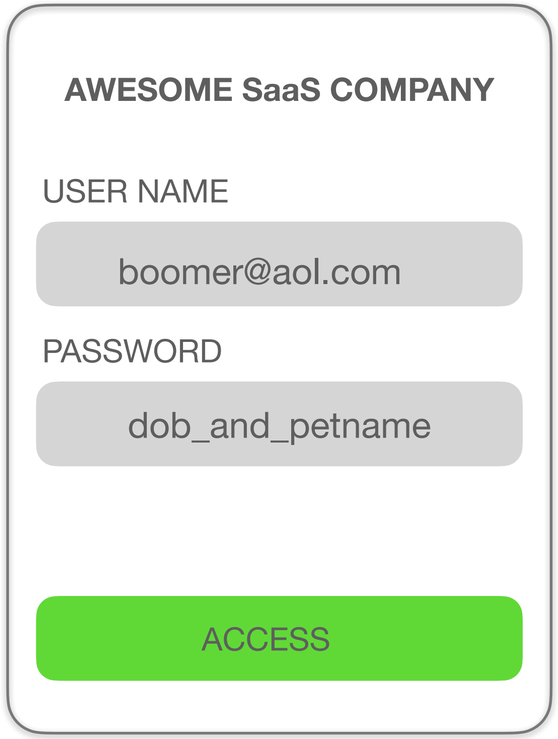
What is a BOT attack?

The use of a script that mimics basic human behavior, whereby computers using “designer” code, stuff password challenge windows with a large volume of username and password combinations, in order to access protected “data”.

What is a BOT attack?

The most common visualization is the login page of a “SaaS” provider.

The BOT has a login, and repeatedly guesses a password.



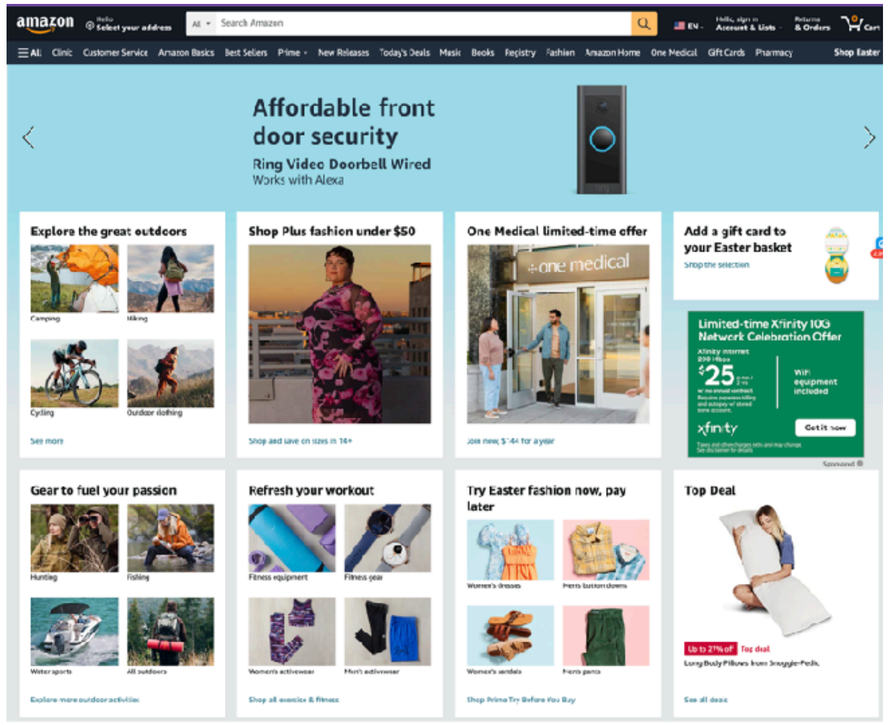
What are common types?

What are types of BOT attack?

- Scraping
- Denial of Service (DDoS)
- Account Takeover (ATOs)
- Transactional Fraud

What are types of BOT attack?

- **Scraping**
- Denial of Service (DDoS)
- Account Takeover (ATOs)
- Transactional Fraud



The BOT reads (scrapes) all of the code on web-pages to gather all the information that they will need for a later malicious attack.

These happen all the time and are usually coordinated by several BOT farms.

What are types of BOT attack?

- Scraping
- **Denial of Service (DDoS)**
- Account Takeover (ATOs)
- Transactional Fraud

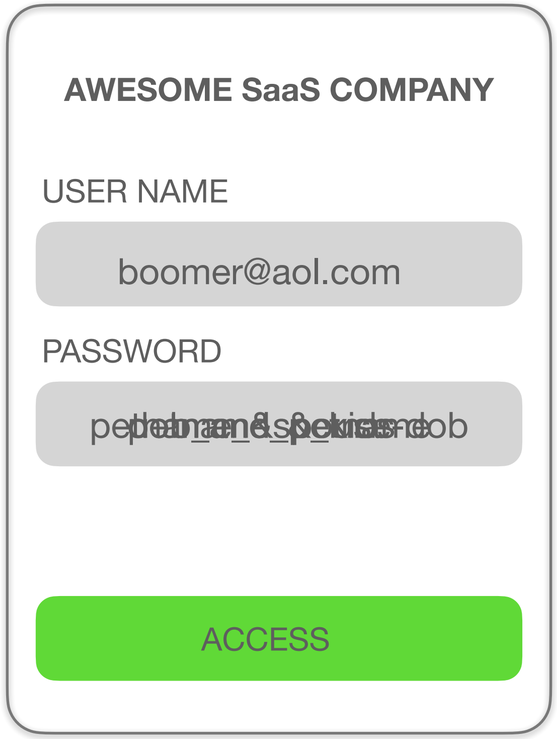
503!

A BOT or group of BOTs act to block access to a property, overwhelming its ability to handle the multitude of concurrent or consecutive requests.

These were popular in the early 2000's and still take place today. They can bring any web dependent business to a halt.

What are types of BOT attack?

- Scraping
- Denial of Service (DDoS)
- **Account Takeover (ATOs)**
- Transactional Fraud

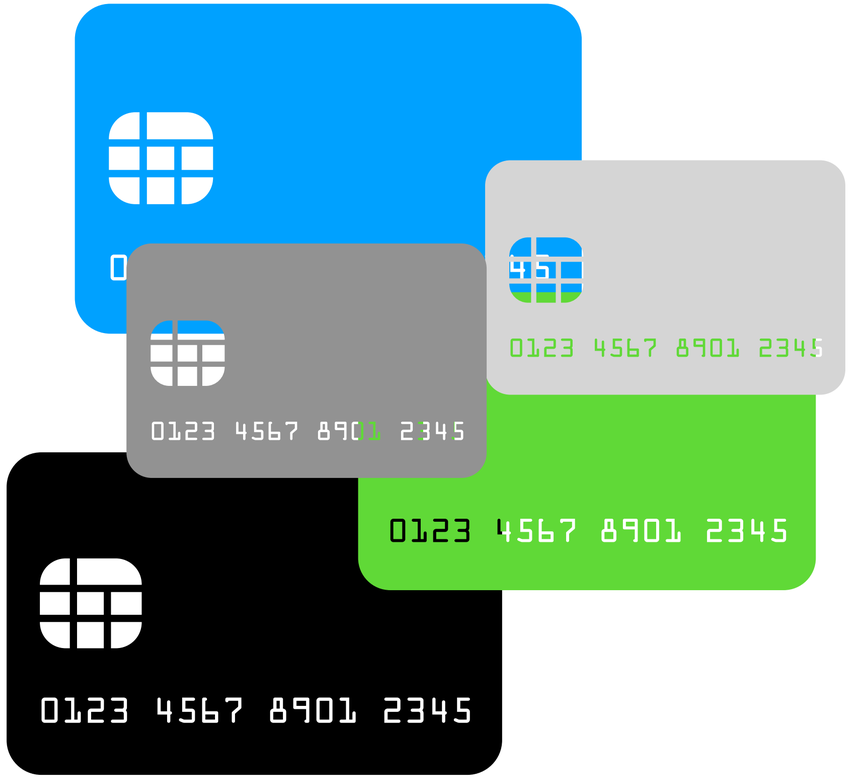


A user name has been stolen, and the BOT is left to guess the password using educated guesses from data obtained in other scraping or identity theft events.

This is persistent in nature and can go on for days until successful.

What are types of BOT attack?

- Scraping
- Denial of Service (DDoS)
- Account Takeover (ATOs)
- **Transactional Fraud**



A BOT uses sensitive information in multiple web locations / services at the same time to mathematically guess a numeric combination.

Based on limited number of permutations of a simple three or four digit code.

ATOs and Transactional BOT attacks

ATO and Transactional BOT attacks

Depend largely on

- Predictability of use
  - User patterns
  - Number of characters and input choice
- Input mechanics
  - Available character choices
  - Standard “CAPTCHA” like systems
- A compromised data element
  - Login name
  - Some PII element

- Birthday dates in a password
- HS / College graduation year
- Use of 2 or 3 initials
- Year of birth in user name
- Year the account was opened
- 26 letters, 10 digits, and 33 specials characters
- Standard reCAPTCHA / CAPTCHA
- 4 digit PINs

Repetition predictability

- Observing a pattern
- Observing patterns of patterns
- Sequences in the entry / validation steps
- Even if encrypted = patterns are engaged

Character	Binary Code	Character	Binary Code	Character	Binary Code	Character	Binary Code	Character	Binary Code
A	01000001	Q	01010001	g	01100111	w	01110111	-	00101101
B	01000010	R	01010010	h	01101000	x	01111000	.	00101110
C	01000011	S	01010011	i	01101001	y	01111001	/	00101111
D	01000100	T	01010100	j	01101010	z	01111010	0	00110000
E	01000101	U	01010101	k	01101011	!	00100001	1	00110001
F	01000110	V	01010110	l	01101100	"	00100010	2	00110010
G	01000111	W	01010111	m	01101101	#	00100011	3	00110011
H	01001000	X	01011000	n	01101110	$	00100100	4	00110100
I	01001001	Y	01011001	o	01101111	%	00100101	5	00110101
J	01001010	Z	01011010	p	01110000	&	00100110	6	00110110
K	01001011	a	01100001	q	01110001	'	00100111	7	00110111
L	01001100	b	01100010	r	01110010	(	00101000	8	00111000
M	01001101	c	01100011	s	01110011	)	00101001	9	00111001
N	01001110	d	01100100	t	01110100	*	00101010	?	00111111
O	01001111	e	01100101	u	01110101	+	00101011	@	01000000
P	01010000	f	01100110	v	01110110	,	00101100	_	01011111

01001000 01100101 01101100 01101100 01101111 00100001 = **HELLO**

What if you were not forced to encode Binary or Hex?

Bound inputs

- Use of limited characters
- Use of language specific characters
- Number of entry data points
- Forced sequence

Character	Binary Code	Character	Binary Code	Character	Binary Code	Character	Binary Code	Character	Binary Code
A	01000001	Q	01010001	g	01100111	w	01110111	-	00101101
B	01000010	R	01010010	h	01101000	x	01111000	.	00101110
C	01000011	S	01010011	i	01101001	y	01111001	/	00101111
D	01000100	T	01010100	j	01101010	z	01111010	0	00110000
E	01000101	U	01010101	k	01101011	!	00100001	1	00110001
F	01000110	V	01010110	l	01101100	"	00100010	2	00110010
G	01000111	W	01010111	m	01101101	#	00100011	3	00110011
H	01001000	X	01011000	n	01101110	$	00100100	4	00110100
I	01001001	Y	01011001	o	01101111	%	00100101	5	00110101
J	01001010	Z	01011010	p	01110000	&	00100110	6	00110110
K	01001011	a	01100001	q	01110001	'	00100111	7	00110111
L	01001100	b	01100010	r	01110010	(	00101000	8	00111000
M	01001101	c	01100011	s	01110011	)	00101001	9	00111001
N	01001110	d	01100100	t	01110100	*	00101010	?	00111111
O	01001111	e	01100101	u	01110101	+	00101011	@	01000000
P	01010000	f	01100110	v	01110110	,	00101100	_	01011111

What if you were not forced to follow a pattern on data entry?
Number, sequence, characters?

Compromised data

- Consolidation of scraped data
- Relating seemingly disparate pieces of data
- Building together the PII puzzle

=

ATO and Transactional BOT attacks

REPETITION PREDICTABILITY	BOUND INPUTS	COMPROMISED DATA
UNIQUE RANDOMNESS	UNLIMITED INPUT	ZERO PII

The ideal MFA solution can't be…

MFA

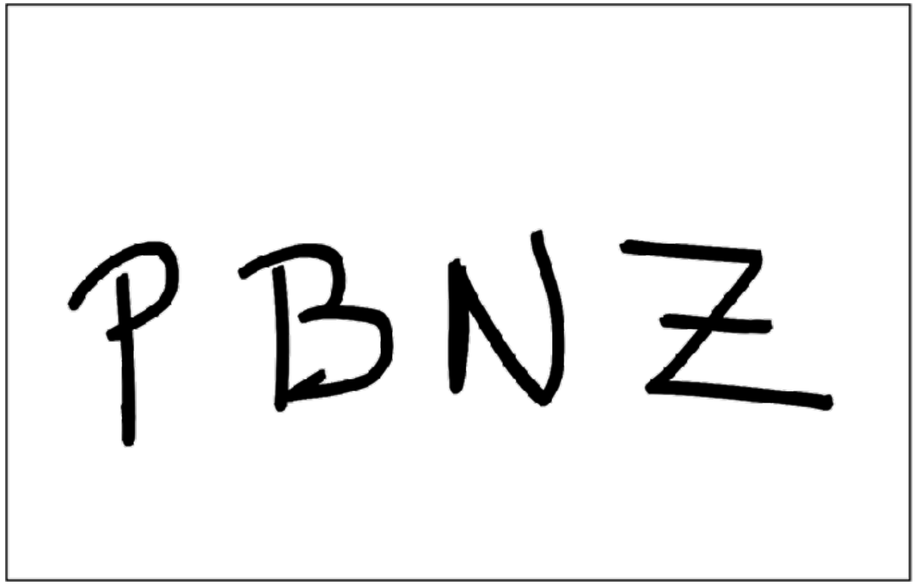
Classic and new factors

	Shared	Stolen	Replicated
Knowledge	✗	✗	✗
Possession	✗	✗	✗
Inherence	✓	✗	✗
Ability	✓	✓	✓
Randomness	✗	✗	✓
Location	✗	✗	✗

Behavioral biometrics

About *written / drawn* passwords…

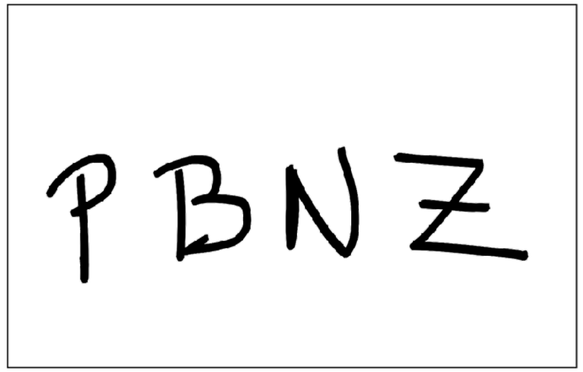
- They are not authenticated as “calligraphy”
- It’s not about “pretty” it is all about “can you repeat it”
- Mathematically, nearly impossible to beat.
- Will “trip” a robot trying to replicate.
- Inherently “random”, yet “predictable”
- Easier to memorize (eg. Your signature)
- May require mental clarity / focus
- Don’t require training. Require proficiency.



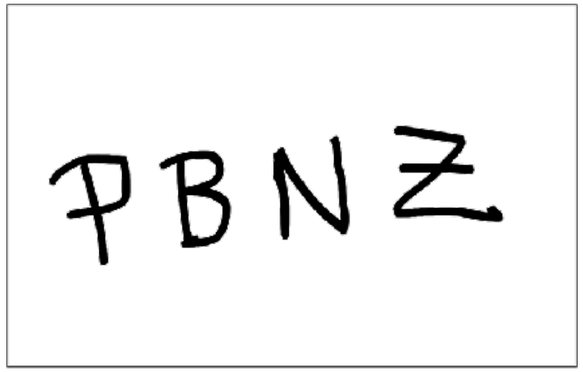
>BNs : 1 odds to hack….
Inherently random

Behavioral biometrics

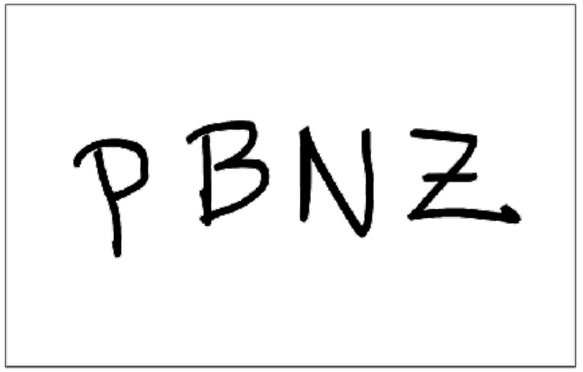
About *written / drawn* passwords…



Example 1



Example 2



Example 3

Same “code”, but not the same..

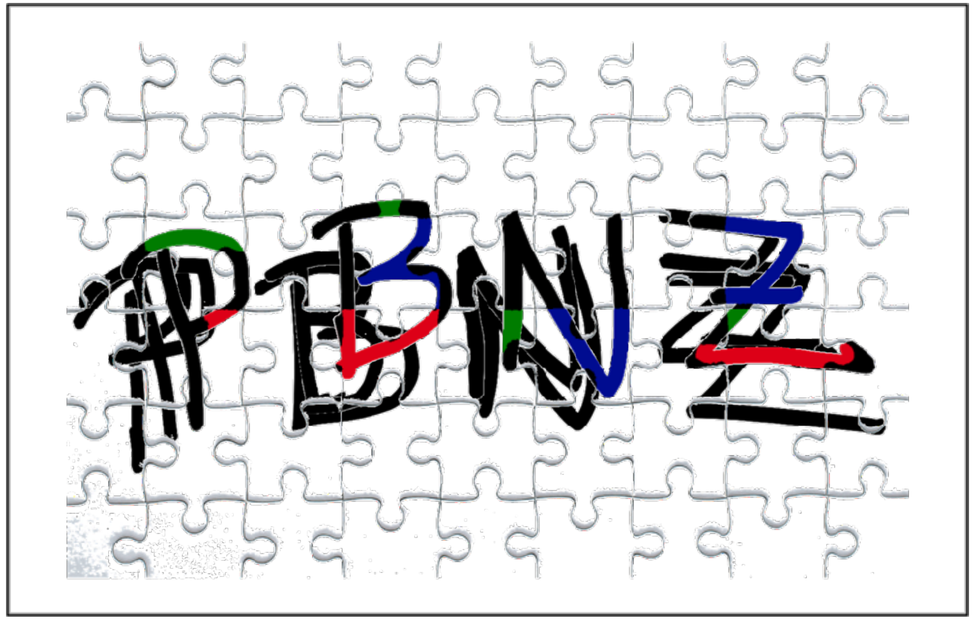
Behavioral biometrics

About *written / drawn* passwords…

It’s not about comparing pictures…

Behavioral biometrics

About *written / drawn* passwords…



- Random
- Inherent
- Ability

It’s about how only you can build a math model puzzle that is NOT a coded image…


DETERRENCE

“Dominate the terrain…”

SUN TZU

Thwarting BOT attacks

Behavioral biometric credentials are a strong deterrent against account takeover (ATO) and transactional BOT attacks because they inject complexity that counter-overwhelms the BOTs

They beat BOTs by NOT playing their game, and being:

- Unique
- Infinite
- Free of personal markers

UNIQUE
RANDOMNESS

UNLIMITED
INPUT

ZERO
PII

Biometric Signature ID

Protecting your data and identity from BOTs.

SOLUTION

Advanced MFA

BSI's Behavioral Biometrics

"Inherence"	"Knowledge"	"Possession"	"Ability"
Awareness	Code / Password	Device	Signature

Physical Biometrics + Other Techs.

Face, Walking, Palmprint, DNA, Veins, Retina, Palm Geometry, Fingerprints

Can be stolen, replicated, or shared.

Most products and solutions meet only one of the MFA requirements.

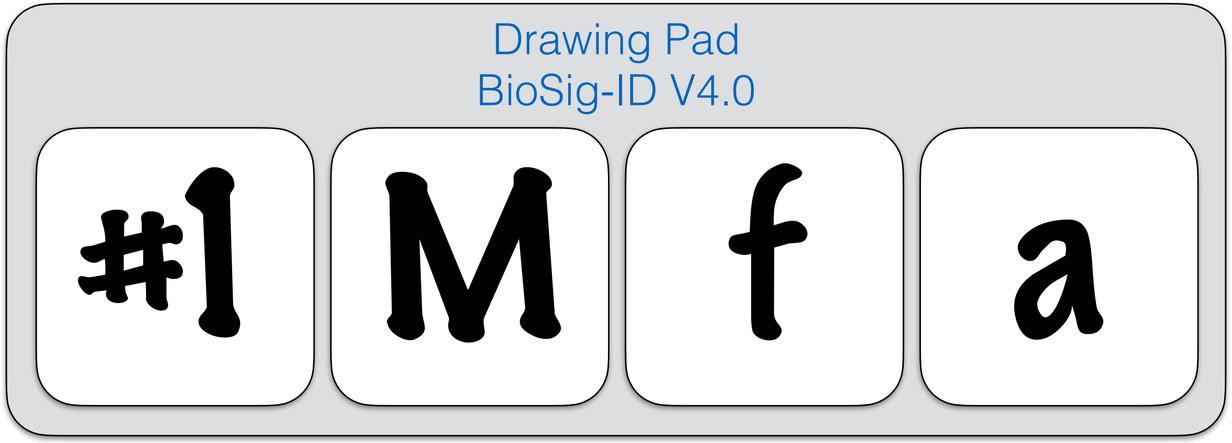
Code / Password

UBI Key

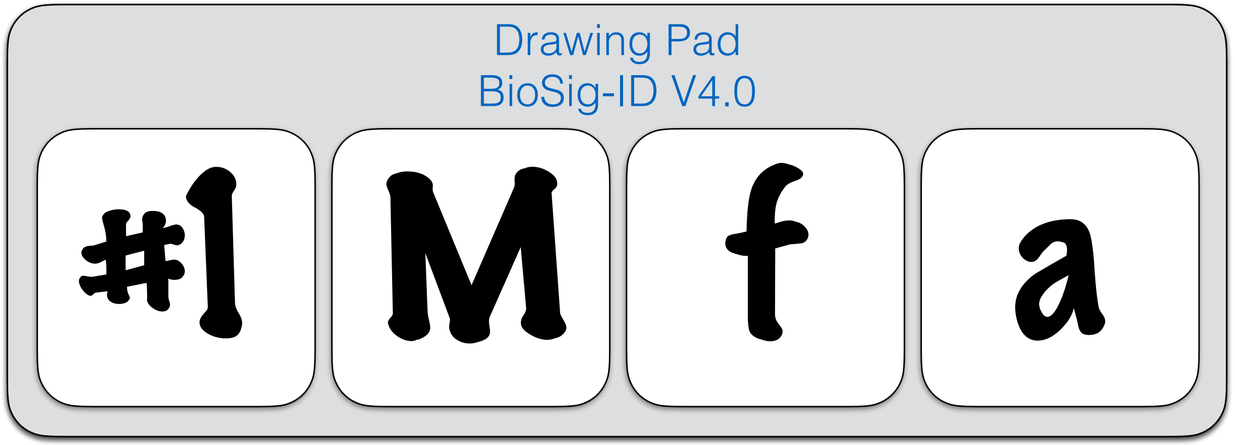
SOLUTION

Passwords that can’t be stolen…

- All-at-once Advanced MFA
- Needs no special hardware
- Has no private identifiable information
- 192 billion to one link to a human
- Linked to user’s state of mind



Unique and robust credentials



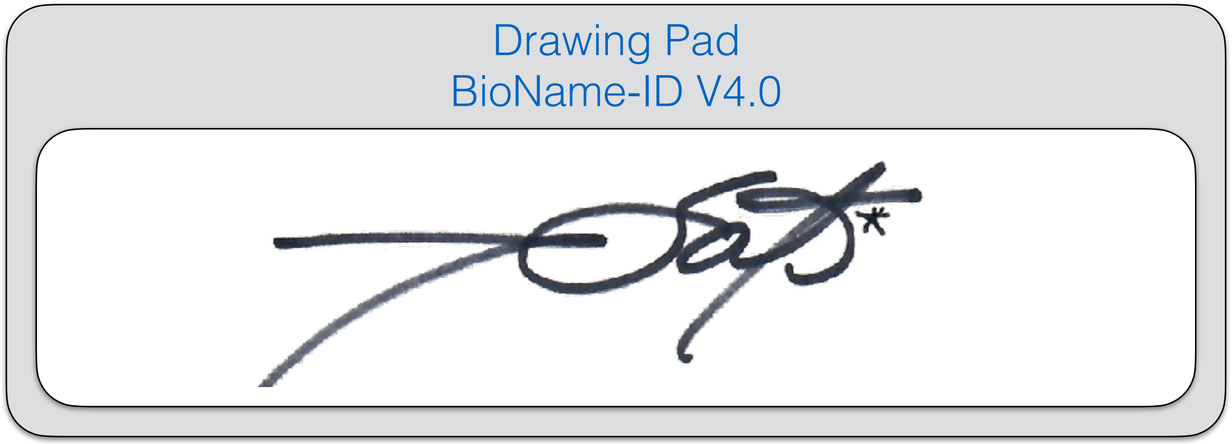
In one single action, the user meets all MFA requirements.

That's it.

The "challenge screen" is presented to the user at any time validation is required in the process.

Using a finger, mouse or stylus, the user writes their password.

Unique and robust credentials



A “signature” instead of a “pin” can also be used for different user experience.

In one single action, the user meets all MFA requirements.

That’s it.

MFA credentials that kill BOTs.

2023