1Kosmos presents... A history of passwords 1960-2021
Inventor: Fernando Corbato

1960

What
Passwords

Why
Protect a mainframe with shared resources

Weakness
Guessing, Stealing, MiTM, Phishing
1973

**What**
Encrypted Passwords (Hashed, CRYPT)

**Why**
Prevent dictionary attacks

**Weakness**
Guessing, Stealing, MiTM, Phishing
1974

What
Smartcards

Why
Secret Storage (Private Key)

Weakness
Cumbersome, Expensive
1984
Bill Gates

What
End of Password Prediction

Why
Passwords Suck
1993

What
Hardware Tokens

Why
Introduction of a possession factor

Weakness
Cumbersome, MiTM, Phishing
2005

What
SMS/e-Mail 2FA

Why
Introduction of a possession factor

Weakness
Delays, reliance on network, SIM-Jacking, phishing, MiTM
2013

**What**
FIDO Alliance

**Why**
Create a second factor authentication protocol

**Weakness**
Requires a first factor, limited platform support
2014

**What**
U2F

**Why**
Make a second factor simpler via USB and NFC

**Weakness**
No mobile-only experience
2016

What
SMS Deprecated by NIST

Why
SMS's can be intercepted or stolen

Weakness
N/A
What
Password + Push Message

Why
Mitigate the risks of email/SMS 2FA

Weakness
Vendor lock-In, dependency on push, difficult to integrate into 3rd party apps
2017

**What**
Identity Proofing

**Why**
Enroll and verify remote identities

**Weakness**
Decoupled from authentication technologies (like FIDO)
2018

What
FIDO2 WebAuthn

Why
Public key cryptography plus biometrics prevent password and 2FA theft

Weakness
Limited platform support, binding requires a username/password
2019

Inventor: 1Kosmos

What
Identity Based Authentication

Why
Authentication needs a strong identity

Weakness
No support for the 1960 MIT mainframe
Strong Authentication with Strong Identity

Secure online services from password-based attacks with a next generation approach to multi-factor authentication that delivers a frictionless user experience.