



Passwordless Authentication

June 12, 2019



Today's web conference is generously sponsored by:



SecureAuth

<https://www.secureauth.com/>



Moderator

Dipto Chakravarty, Chairman of Security COE, IoT Community

Dipto Chakravarty is the author of three best-selling books on computer architecture and security from McGraw-Hill and Wiley that have been translated in five languages. He has 11 patents to his credit in AI, security and cloud, holds a M.S in Computer Science from U. of Maryland, GMP from Harvard Business School, and EMBA from Wharton School U. Penn. He is currently the Chairman of Security, Privacy and Trust COE for IoT Community, and board member at RANK Software.



Speaker

Mike McKinzie, Solutions Advisor, Swivel Secure

Mike McKinzie is a Solutions Advisor with Swivel Secure, a leading provider of 2FA/MFA solutions. Prior to joining Swivel Secure, Mike operated a boutique Security practice focused on Cyber Security serving Fortune 1000 companies. In addition, Mike has worked in Security Operations with a prominent Casino operator in Las Vegas, as a Systems Engineer with PGP, taught an Information Security course at Cal State, Fullerton and held various technical and security positions with a nationwide accounting firm. He holds a B.A from UC Irvine, earned his CISSP designation and is an active member of ISSA, Infragard and the ISF.



ISSA

Information Systems Security Association
International

www.issa.org

ISSA Thought Leadership Webinar

Passwordless Authentication

June 12, 2019

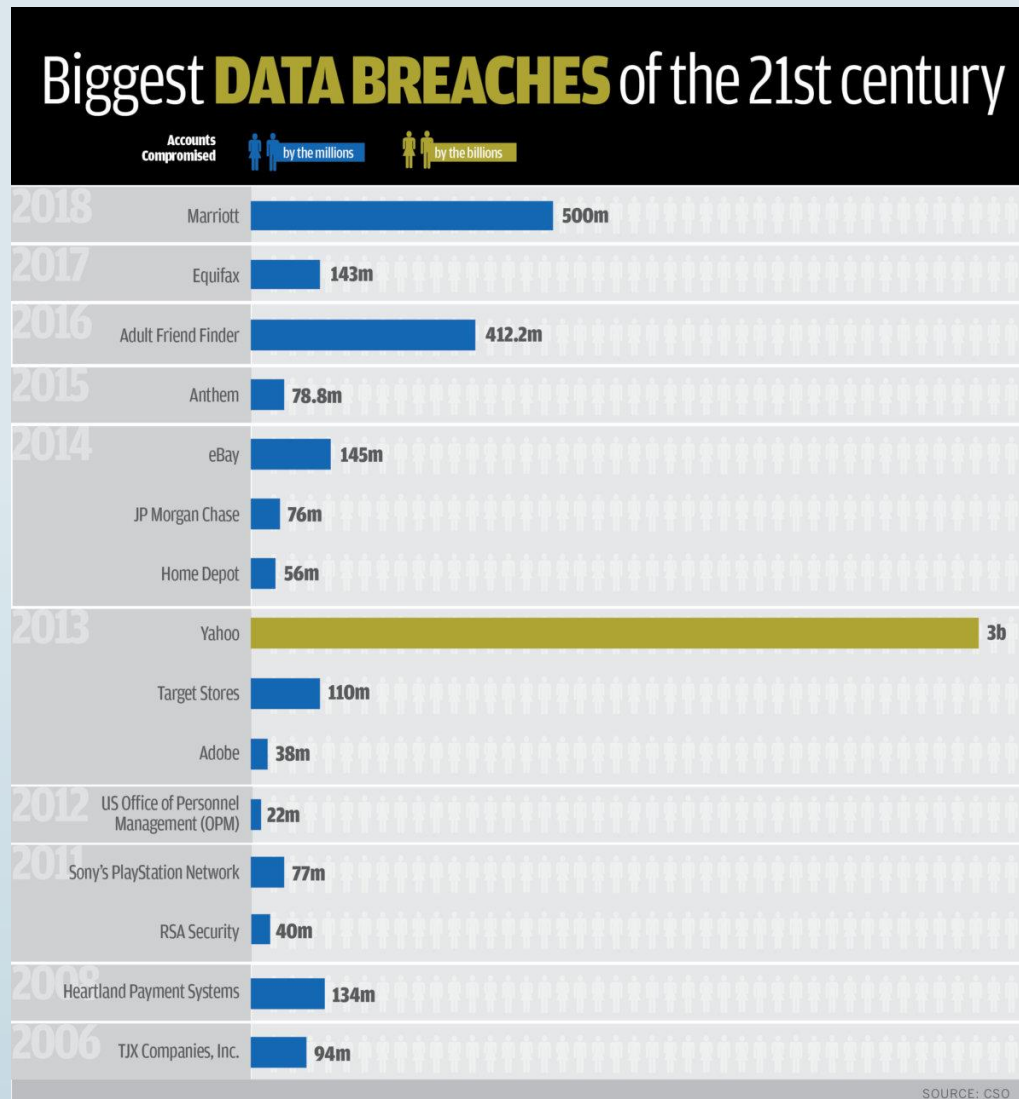
Passwords – In production a long time

- Passwords Used In Roman Times – Called a “Watchword”
- 101st Airborne D-Day
 - ❑ The Cricket (Identification/Authentication)
 - ✓ Friend or Foe
 - ❑ Challenge: “Flash” & “Thunder”
- 1961 CTSS MIT
 - ❑ Shared System, Single Disk File
 - ❑ Fernando Corbato (Professor MIT)
 - ❑ “Passwords are NOT a super high level of security, but stop people from casually snooping” – F.C.
- NIST says less than 10 Characters is weak ; password entropy ; most sites 6-9 Characters
- Passwords: Computer Culture, Rapid Deployment & Costs!



Password Risk

➤ Maybe we need to consider alternatives?



Password = \$\$\$

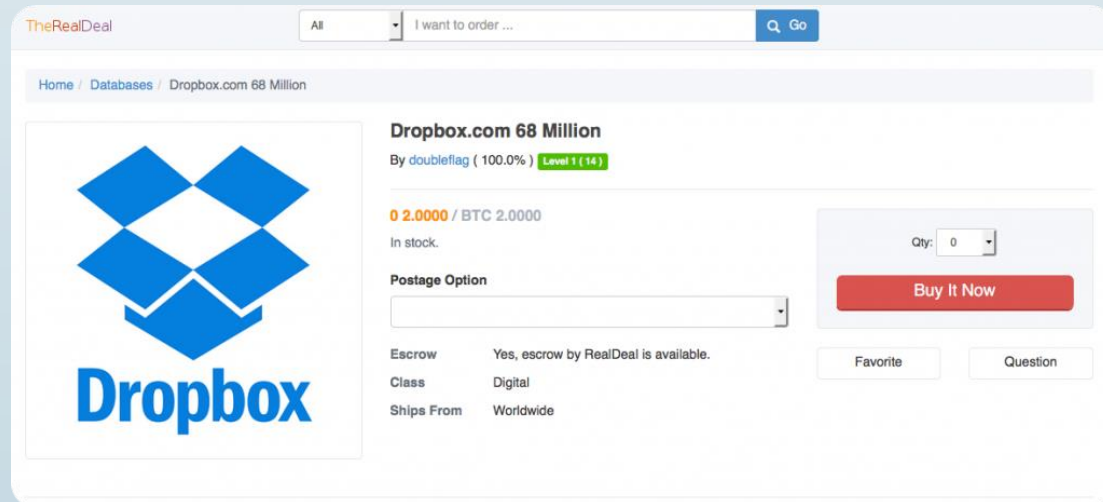
➤ Maybe we need to consider alternatives?

❑ Verizon Data Breach Reports

- ✓ 81% of hacking related breaches due to stolen/weak passwords
- ✓ 70% Employees Re-use passwords at work
- ✓ Millennials 18-31| 87% Re-use passwords

❑ Dropbox, 60 Million User Credentials stolen

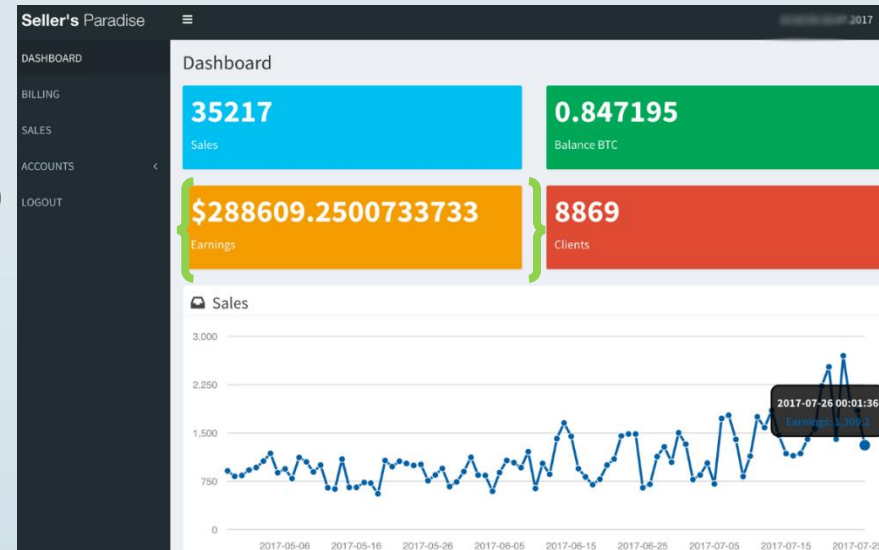
- ✓ Cause: Employee re-used a password
- ✓ Then:



The screenshot shows a marketplace listing for 'Dropbox.com 68 Million' credentials. The listing includes the Dropbox logo, the price '0 2.0000 / BTC 2.0000', and a 'Buy It Now' button. The seller is 'doubleflag' with a 100.0% rating. The listing also shows 'In stock', 'Postage Option', 'Escrow' status, 'Class' (Digital), and 'Ships From' (Worldwide).

The Market for Passwords

- 100B since 2010
- Hackers on average earn \$41.47/Hour
- Everyone's details have value
 - Children
 - Medical Record: \$1,000
 - Credit Card Details: \$22.39
 - DL: \$20
 - Netflix: \$3.05
 - BTW: Good Credit Pays!
 - ✓ \$150/Record vs Avg



Why Are We Still Using Passwords?

➤ Costs?

- Easy to deploy for Vendors and for Organizations
 - ✓ Ponemon: \$148 per compromised record
 - ✓ Increasing each year
- Product solutions have to be purchased, and managed; users educated and supported

➤ Practical Application

- Hybrid IT – password auth is omnipresent
- Passwords can be updated; entropy
- Portability
- MFA, multiple factors may be needed i.e. PIN, Password
- Legacy Apps/Systems

Authentication Utopia?



-
- Admins want it to just work; Users want it to just work
 - How do we achieve this?
 - ✓ SSO/IAM
 - ✓ Context-Aware Auth, “Friction-less”
 - ✓ Biometrics
 - ✓ FIDO2/U2F



ISSA

Information Systems Security Association
International

www.issa.org

QUESTIONS?



Speaker

**Stephen Cox, Vice President and Chief Security Architect,
SecureAuth**

Stephen Cox is a technology veteran with nearly 20 years in the IT industry, including more than 10 years leading cybersecurity software development teams. A key player in some of the most influential IT security firms in the world, he is recognized as an expert in identity, network and endpoint threat detection, as well as an accomplished software architect.

As Vice President and Chief Security Architect at SecureAuth, Stephen helps drive the strategy, vision and development for the company's products and solutions. Prior to SecureAuth, Stephen worked at FireEye/Mandiant, RSA, VeriSign, Northrop Grumman and America Online. He holds a Master of Science in Software Engineering and a Bachelor of Science in Integrative Studies, both from George Mason University.



ISSA

Information Systems Security Association
International

www.issa.org

ISSA Thought Leadership Webinar

Passwordless Authentication

June 12, 2019



the password has become a
"kind of a nightmare"

Prof. Fernando J. Corbato



The Password Is No Longer Acceptable, But...

- Identity Sprawl in a Cloud World
- Long Tail of Legacy
- Rise of Hybrid Environments
- What Lies Beyond 2FA?

Internal Network On-Prem



Internal Users



Internal Apps



User Repository

Identities, everywhere...



- **Digital transformation:**
not buzz, it's real



- **Modern organizations:**
hybrid of on-premises and cloud



- **Identity:**
binds everything together

Credential Stuffing: Paying for Our Mistakes



Attacker obtains cache of stolen credentials



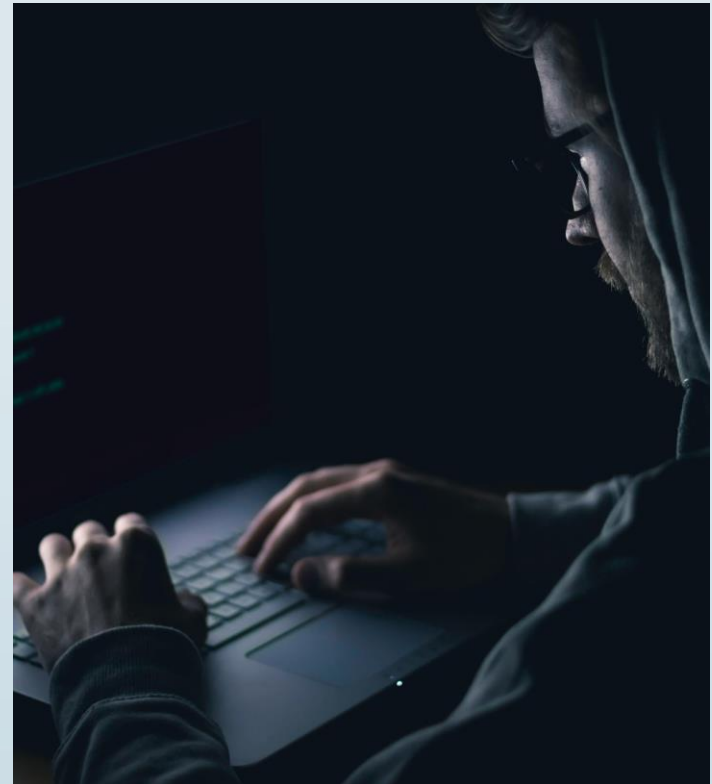
Attacker uses automation tools to “stuff” credentials into resources



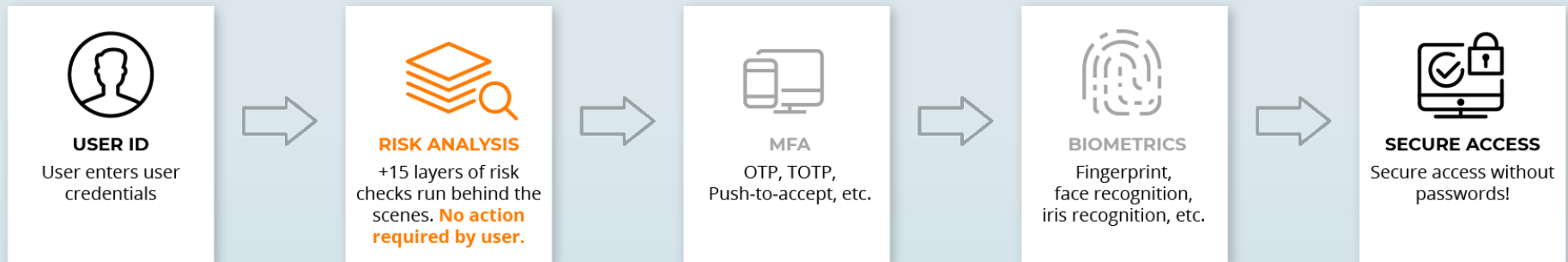
Relies on users reusing passwords



Distributed nature difficult to defend



Passwordless Authentication in Practice



Risk Analysis in Identity Security

Recognition of device

Location the request is coming from

Impossible travel event identified

Group membership and attribute checking

Check IP address reputation against lists

Request coming from a anonymous proxy trying to hide IP

Absorb any 3rd party risk score in the authentication process

Block access requests from unknown phone carriers

Block access requests from varying phone types (e.g. VoIP)

Know if phone has recently been ported (SIM swapped to new phone)

Check IPs against real-time threat intelligence feeds of malicious IPs

Identify abnormal user behavior that could signal attacker presence

Device Recognition

Geo-Location

Geo-Velocity

Directory Lookup

IP White/Black List

Anonymous Proxy

3rd Party Risk Score

Network Carrier

Phone Type

Porting Status

Malicious IPs

Behavior Analysis

If it's not usable, it's not secure.

-- Jared Spool



➤ Multi-Layered Risk Analysis



➤ Single Sign On



➤ User Self Service

<https://twitter.com/jmspool>



ISSA

Information Systems Security Association
International

www.issa.org

QUESTIONS?