Update on IdM for Research: What's new since SC17?

Von Welch

Director, IU CACR - Advisor for Research, Incommon Steering Committee

SC18

November 14, 2018

CENTER FOR APPLIED CYBERSECURITY RESEARCH

PERVASIVE TECHNOLOGY INSTITUTE

Update on IdM for Research:

~~What's new since SC17?~~

Some Predictions on the Future of IdM

Von Welch

Director, IU CACR - Advisor for Research, Incommon Steering Committee

SC18

November 14, 2018

CENTER FOR APPLIED
CYBERSECURITY RESEARCH
PERVASIVE TECHNOLOGY INSTITUTE

About this Talk...

Covering both Identity Management (IdM) and Identity & Access Management (IAM)

Update since my talk at SC17:
https://doi.org/10.6084/m9.figshare.5687086.v1

Update since my talk at SC16:
https://dx.doi.org/10.6084/m9.figshare.4282532

Which was update from SC15:
https://dx.doi.org/10.6084/m9.figshare.3118135

This year, something a little different...

We continue to make progress, but this last year seems more evolutionary than revolutionary.

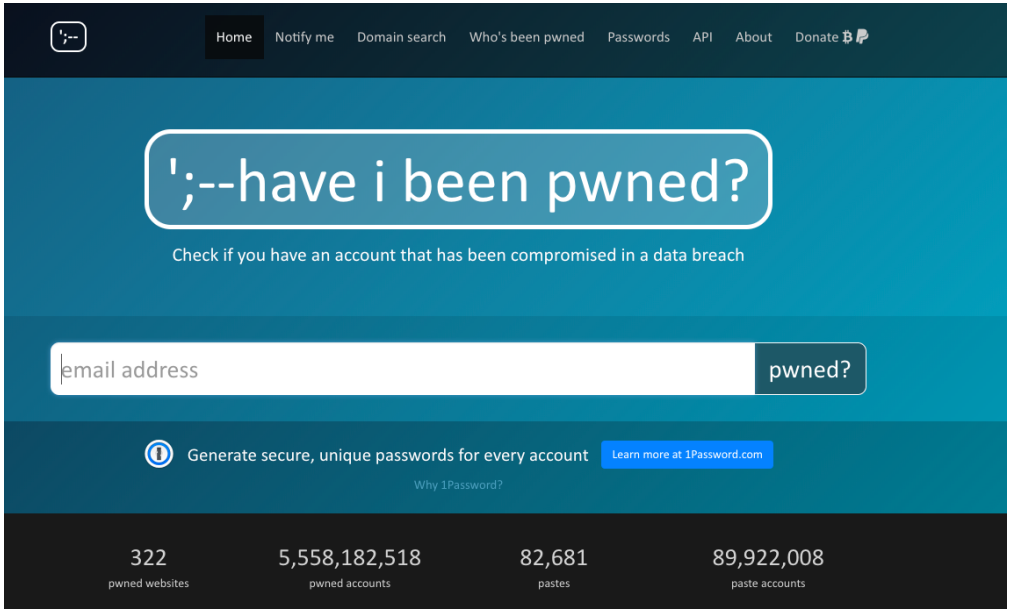
Hence, I'm going to do something a little different and try to do some predictions.

Some observations….

We all have a bunch of passwords now...

The Password DB Breach….

Has made password reuse by users the biggest enemy.



https://haveibeenpwned.com/

Silicon 1, Carbon 0

Trying to have carbon-based lifeforms remember strong passwords that a silicon-based computer cannot crack is hard.

Trying to have carbon-based remember dozens of different strong passwords is impossible.

Time to crack...

8 characters	1 minute
9 characters	2 hours
10 characters	1 week
11 characters	2 years
12 characters	2 centuries

https://blog.codinghorror.com/your-password-is-too-damn-short/

Old heuristics are no longer working...

NIST Special Publication 800-63

Revision 3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Proposed NIST Password Guidelines Soften Length, Complexity Focus

Author:
Michael Mimoso
May 3, 2017 / 1:55 pm
2 minute read
Share this article:

https://threatpost.com/proposed-nist-password-guidelines-soften-length-complexity-focus/125393/

Conclusion: We are not very good at authenticating humans over networks.

https://www.pexels.com/photo/boy-wearing-blue-t-shirt-using-black-laptop-computer-in-a-dim-lighted-scenario-159533/

To the (temporary) rescue...

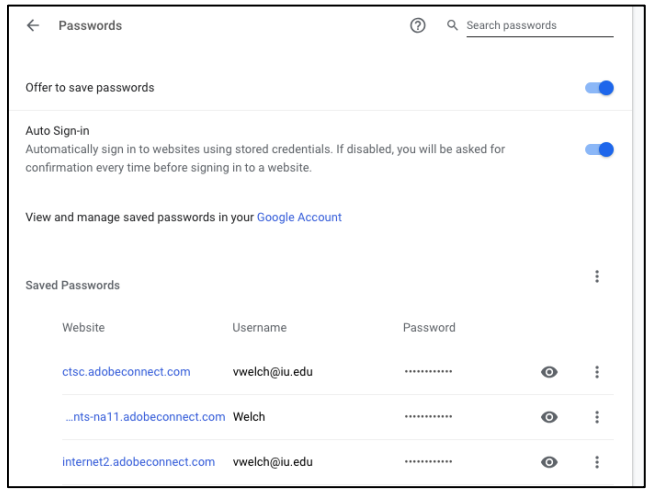
https://www.pexels.com/photo/antique-armor-black-and-white-chrome-350784/

The Rise of the Password Safes

Standalone and in-browser

LastPass

1Password



Chrome

The Rise of SSO

InCommon®

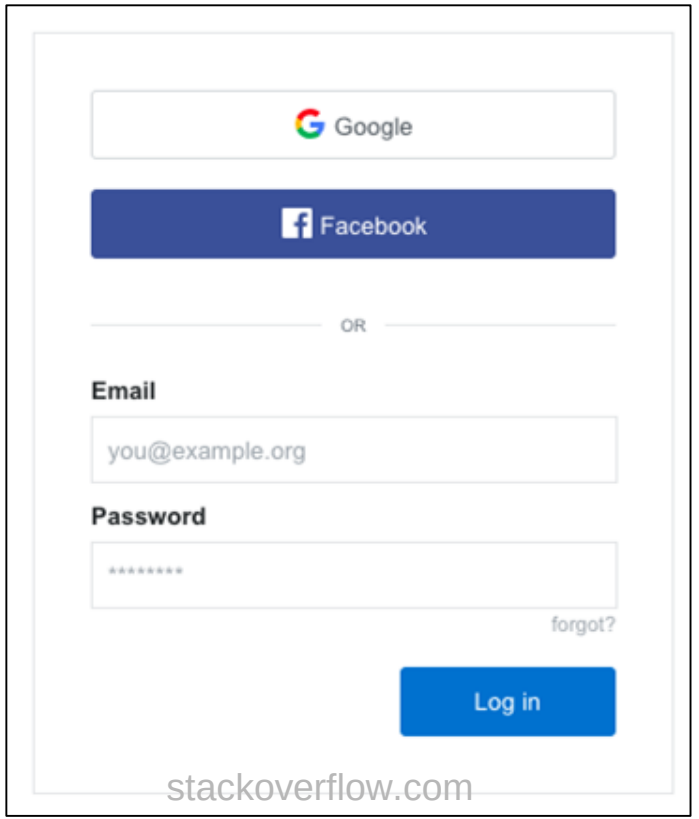
ORCID

eduGAIN

Globus Auth

CILogon

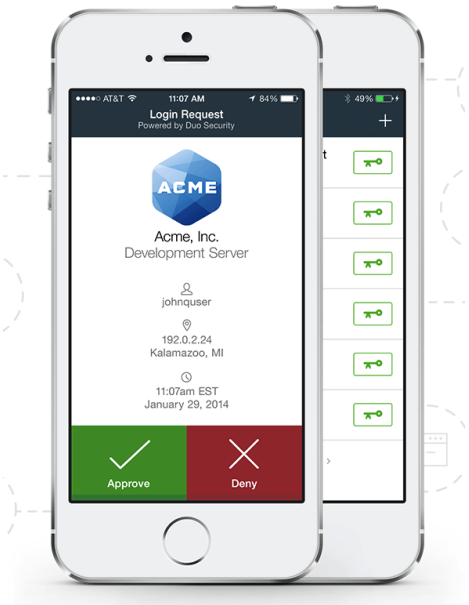
OAUTH

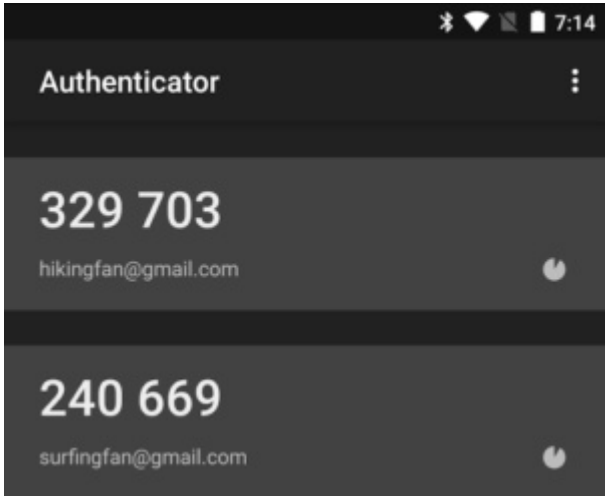


Long Live the Password?

https://www.troyhunt.com/heres-why-insert-thing-here-is-not-a-password-killer/

Smart phones have become common and make for great two-factor devices….

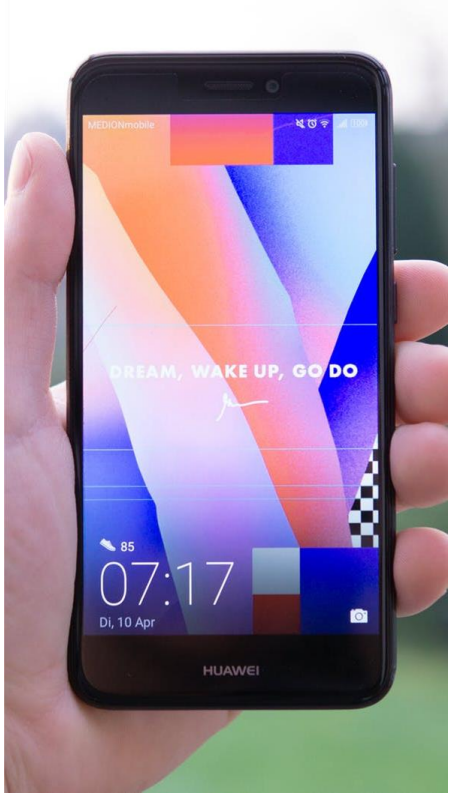




Google Authenticator

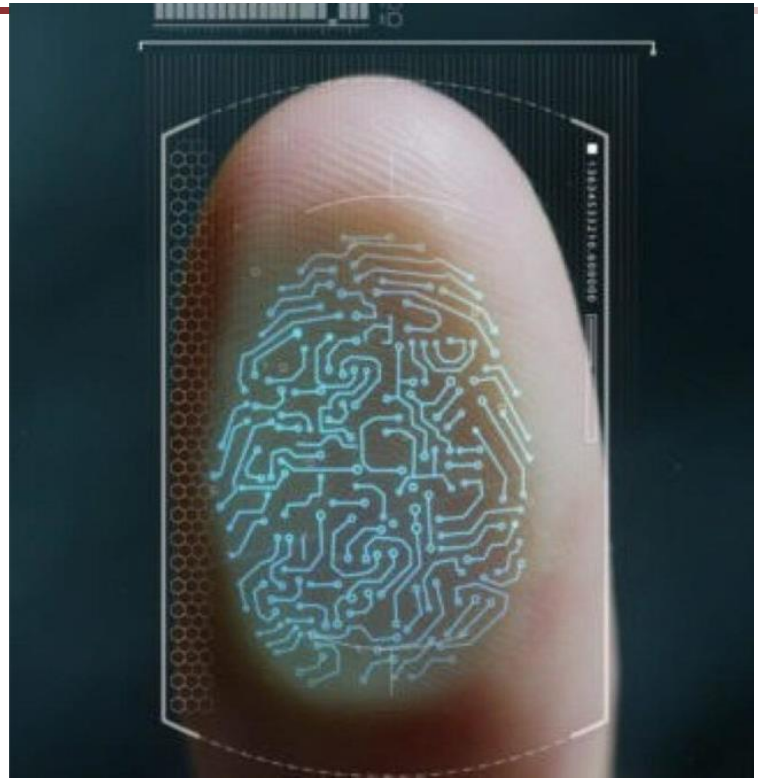
duo.com

And they have given biometrics a use...



https://www.pexels.com/photo/black-huawei-android-smartphone-1036619/

+

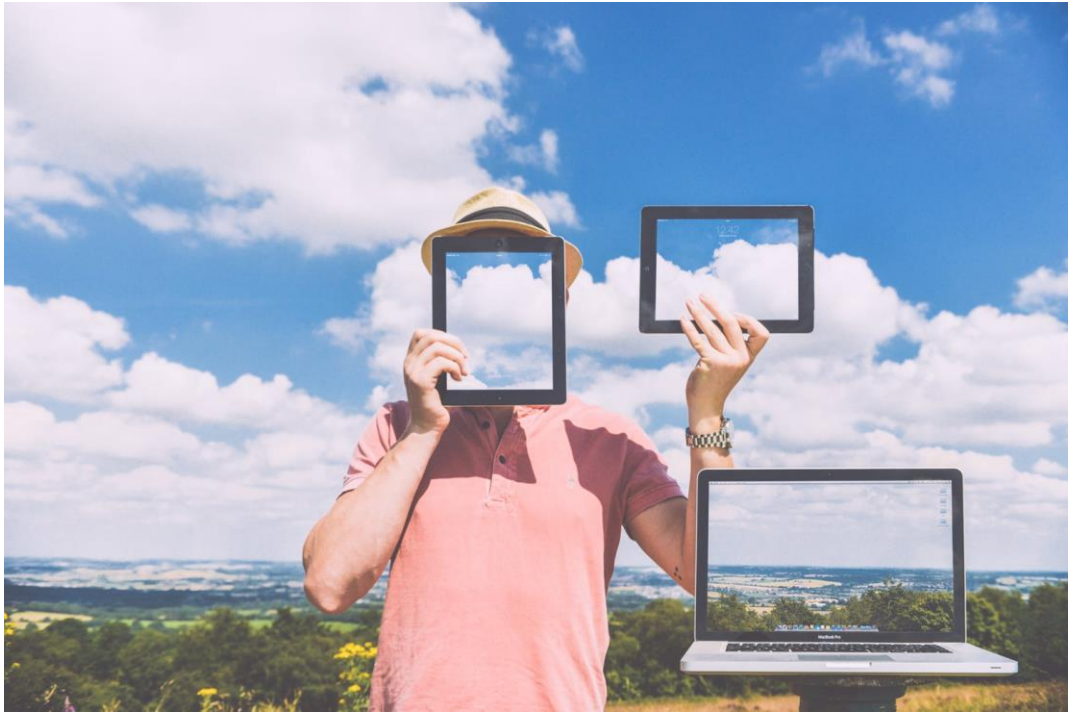


https://news.utexas.edu/2018/05/03/new-survey-on-consumer-attitudes-toward-biometric-technology/

IOT: The death of the keyboard?

https://www.pexels.com/photo/round-grey-speaker-on-brown-board-1072851/

Rise of Cloud…



Two IdM implications:

1. Agents that can operate on our behalf
2. Need to authorized B2B collaboration on our behalf

https://www.pexels.com/photo/nature-laptop-outside-macbook-6508/

“It's tough to make predictions, especially about the future.” - Yogi Berra

https://www.pexels.com/photo/selective-focus-photography-of-water-globe-with-tree-illustration-1046209/

The Death of End-to-end Authentication

Two-factor will not live forever

I don’t know how, but history says it will fall.

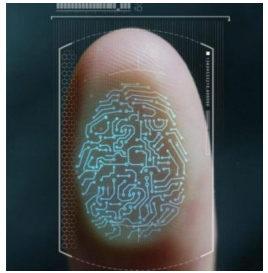
https://www.extremetech.com/extreme/269121-this-tool-can-hack-your-accounts-even-with-two-factor-authentication

Biometrics and IOT will win

Too convenient

Security will get better

Will not be perfect, but will be good enough



Set up multiple users for your speaker

You can link up to 6 people's voices with Voice Match to a single speaker. After you link your voice, you can use voice commands to listen to personalized media.

Link your voice

To link your voice with Voice Match, you must link one Google Account. If you have multiple Google Accounts, you can choose which account you want to use.

1. Open the Google Home app .
2. Tap Account .
3. Verify that the Google Account that is listed is the one linked to Google Home. To switch accounts, click the triangle to the right of the account name and email address.
4. Tap **Settings** > **Assistant** tab > **Voice match**.
5. Make sure any devices you want to link your voice to are checked.
6. Tap **Continue** > **I agree.**
7. Follow the steps.

Bifurcated Authentication

Collection of local avatars we will authenticate to with biometrics.

https://www.android.com/phones/ - Internet Explorer

Bifurcated Authentication

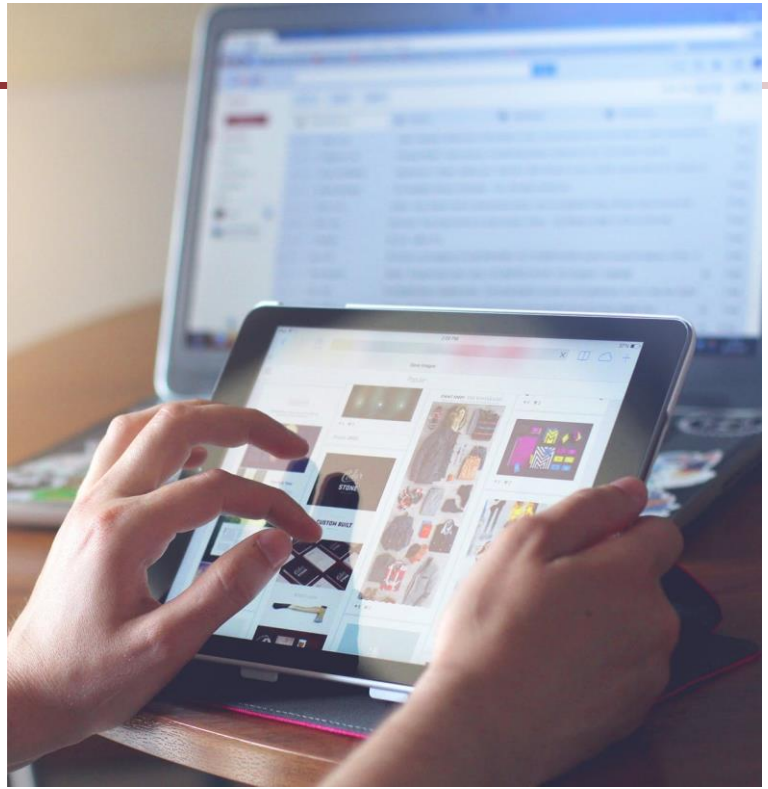
Those avatars will then use strong authentication with the rest of the world on our behalf.

https://www.pexels.com/photo/sky-earth-galaxy-universe-2422/ - https://www.sciencemag.org/news/2013/08/quantum-cryptography-safe-again

Ramifications

The device as a first-class IdM entity...

SSO and IdM systems will need to to get used to authenticating devices authorized by people, rather than people.



https://www.pexels.com/photo/laptop-technology-ipad-tablet-35550/

Password Safes

In-browser password safes will become “invisible” creating strong authentication to websites without human involvement.

Other passwords safes will go the way of the command-line: a tool for the technological edge cases.

Re-enrollment will grow as a problem

Reddit Encounters Hack into its Intermediate Password Reset System

Reddit, which recently conducted a probe inside the office regarding an infiltration into its platform by cyber miscreants, has given out the results stating some unknown hacker managed accessing its intermediate system of password reset.

As accords to the company, although the hacker managed gaining admission into its e-mails recovered through password and which its intermediate software supplier Mailgun dispatched, the hacker could not gain admission into Reddit's computers alternatively the electronic mail accounts of any Redditor. At present, Reddit in cooperation with Mailgun is trying to identify each of the affected accounts.

https://www.spamfighter.com/News-21331-Reddit-Encounters-Hack-into-its-Intermediate-Password-Reset-System.htm

Thank you

vwelch@iu.edu

Thank yous

NSF, DOE

Eric Schmidt, Google,
for seeds of these ideas

Pexels.com for images.

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov