RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: MBS-R02

IMPROVING MOBILE AUTHENTICATION FOR PUBLIC SAFETY AND FIRST RESPONDERS

William Fisher

Security Engineer
National Cybersecurity Center of Excellence
@Billfshr

LET'S TALK ABOUT AUTHENTICATION

Authentication impacts users

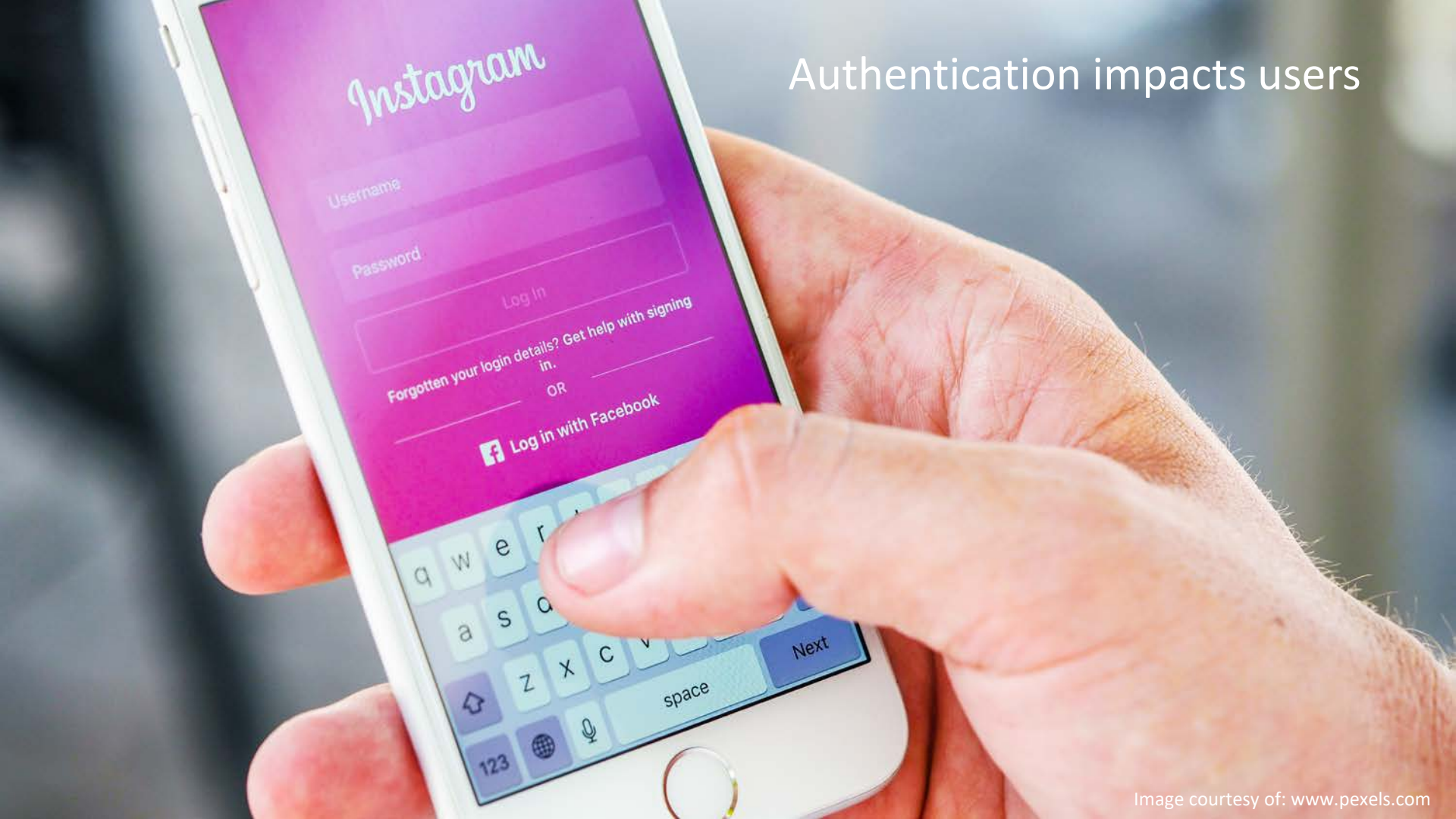
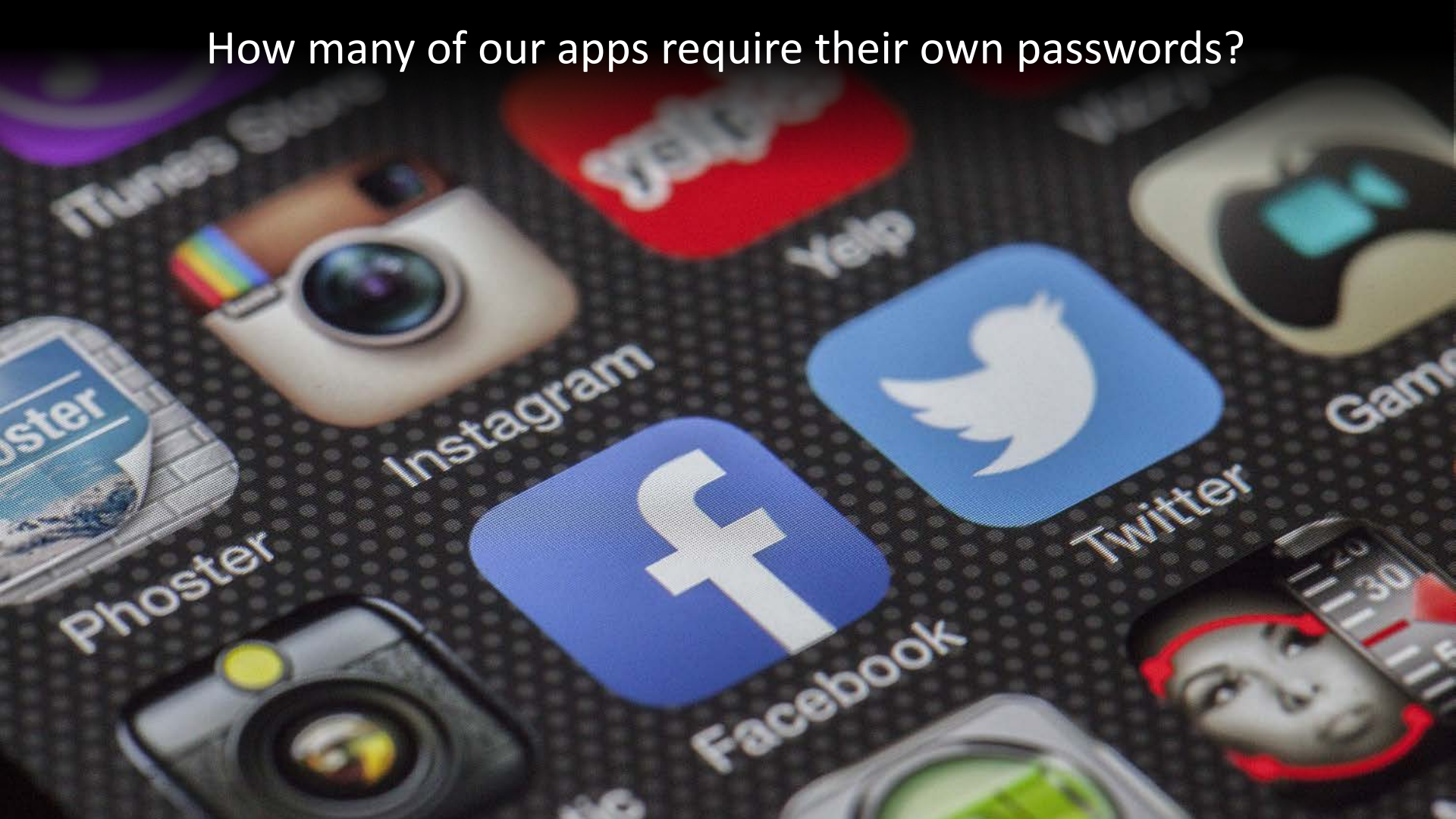


Image courtesy of: www.pexels.com

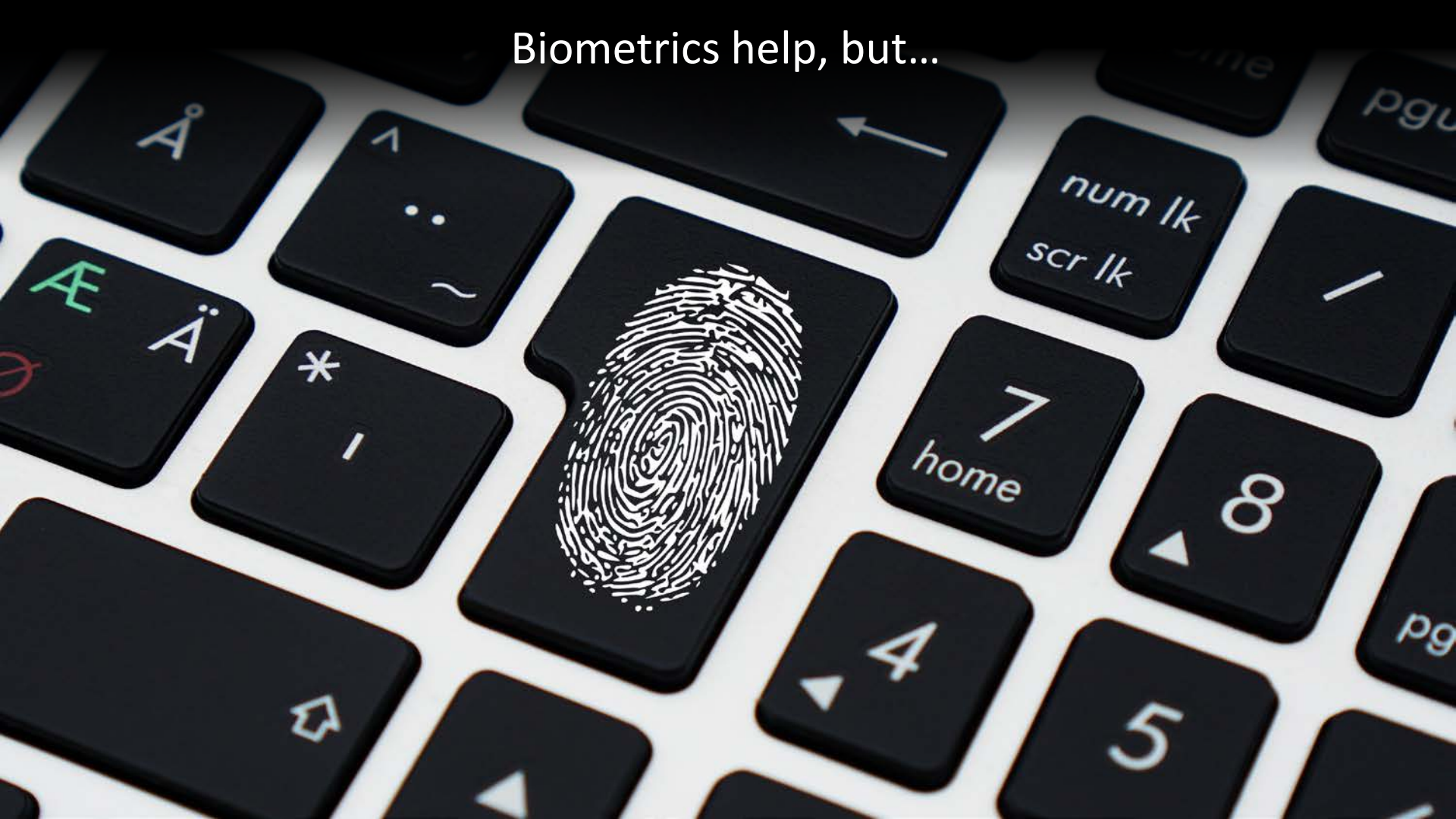
How many of us use Android or iOS devices daily for work?

Image courtesy of: www.pexels.com

How many of our apps require their own passwords?



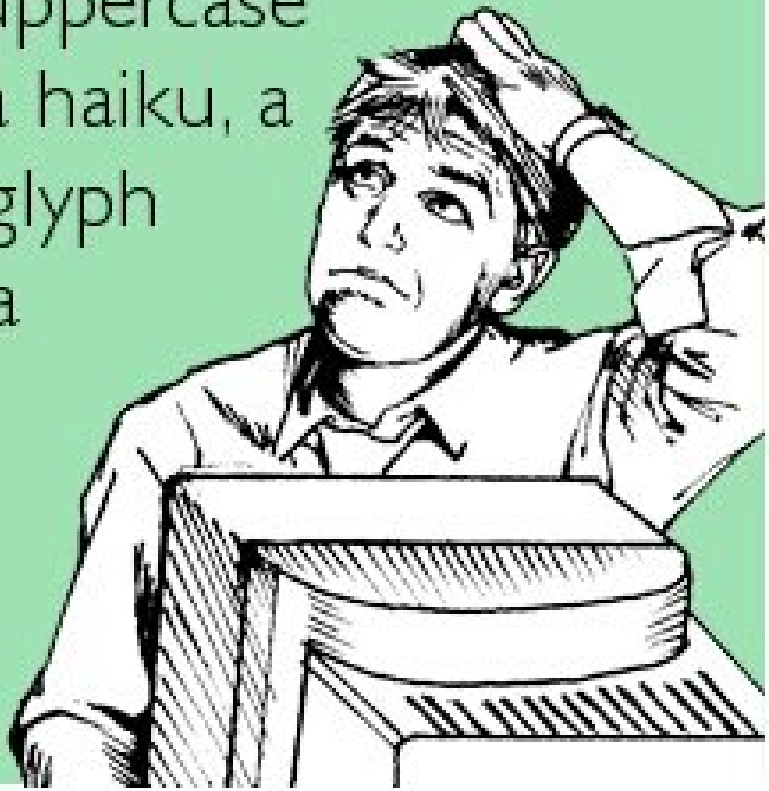
Biometrics help, but…



5am: Please re-enter your password.

Image courtesy of: www.imgflip.com

Sorry, but your password must contain an uppercase letter, a number, a haiku, a gang sign, a hieroglyph and the blood of a virgin.



someecards
user card


space
return
ABC
123
ENG
abcd

We know this…

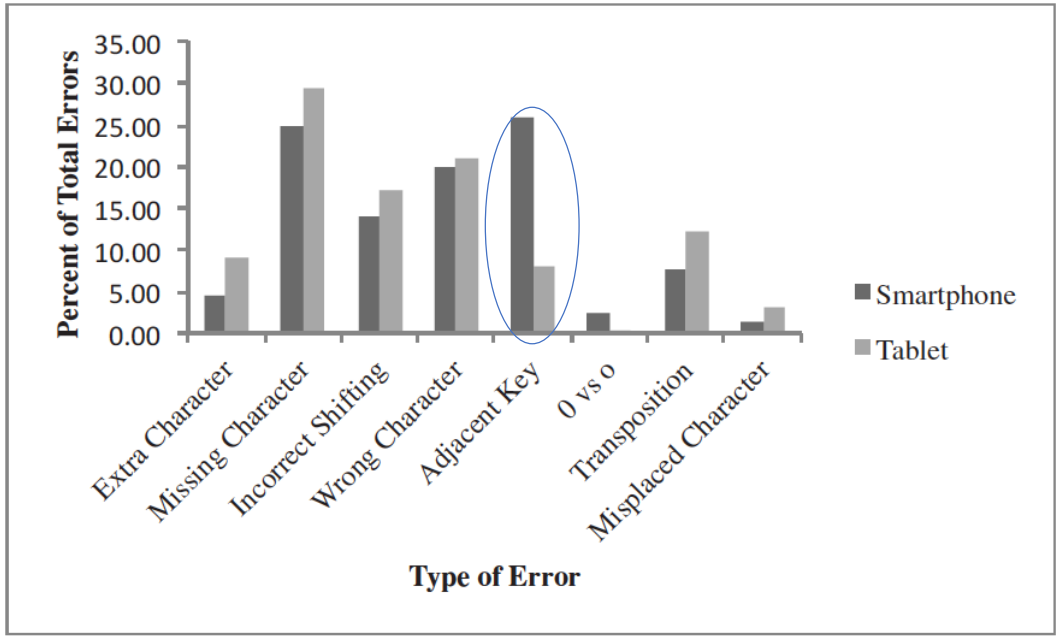


Fig. 6. Percentages of entry errors by error category and device

Greene, K. K., Gallagher, M. A., Stanton, B. C., Lee, P. Y.: I Can't Type That! P@$$w0rd Entry on Mobile Devices. In: Human Aspects of Information, Security, Privacy, and Trust. Lecture Notes in Computer Science, Vol. 8533, pp 160-171. (2014)

What do we get for our troubles?

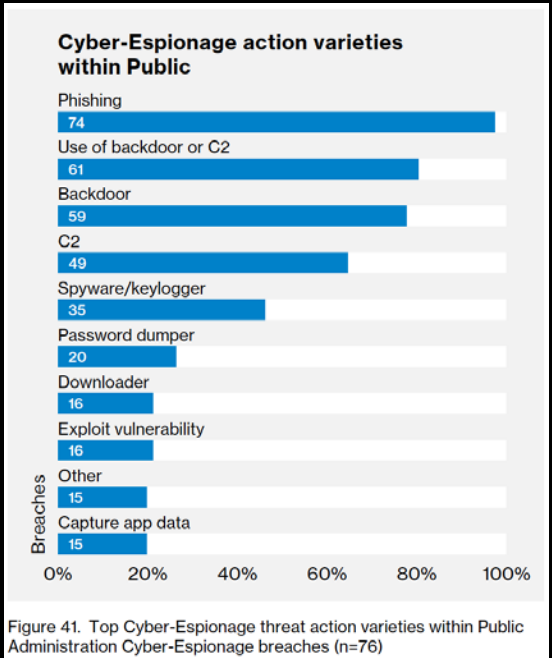
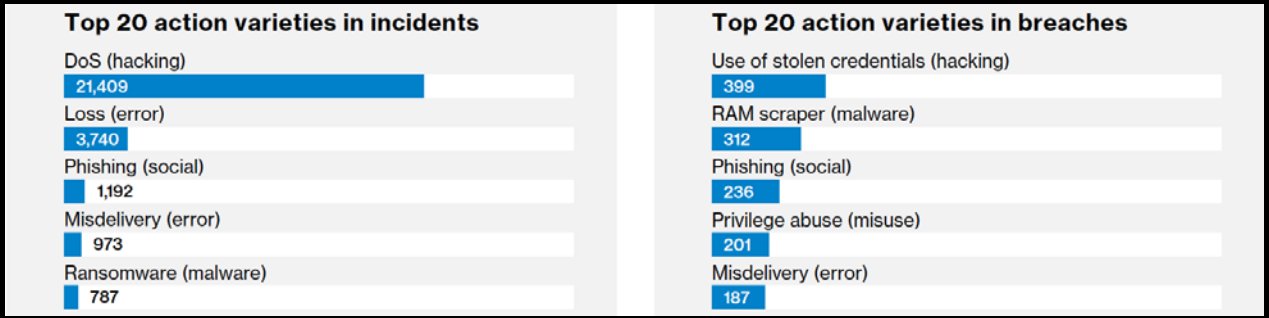


Figure 41. Top Cyber-Espionage threat action varieties within Public Administration Cyber-Espionage breaches (n=76)



Not much in the way of security…

All tables from the Verizon 2018 DBIR https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Image courtesy of: abc

LETS CONSIDER CONTEXT!

At the office?

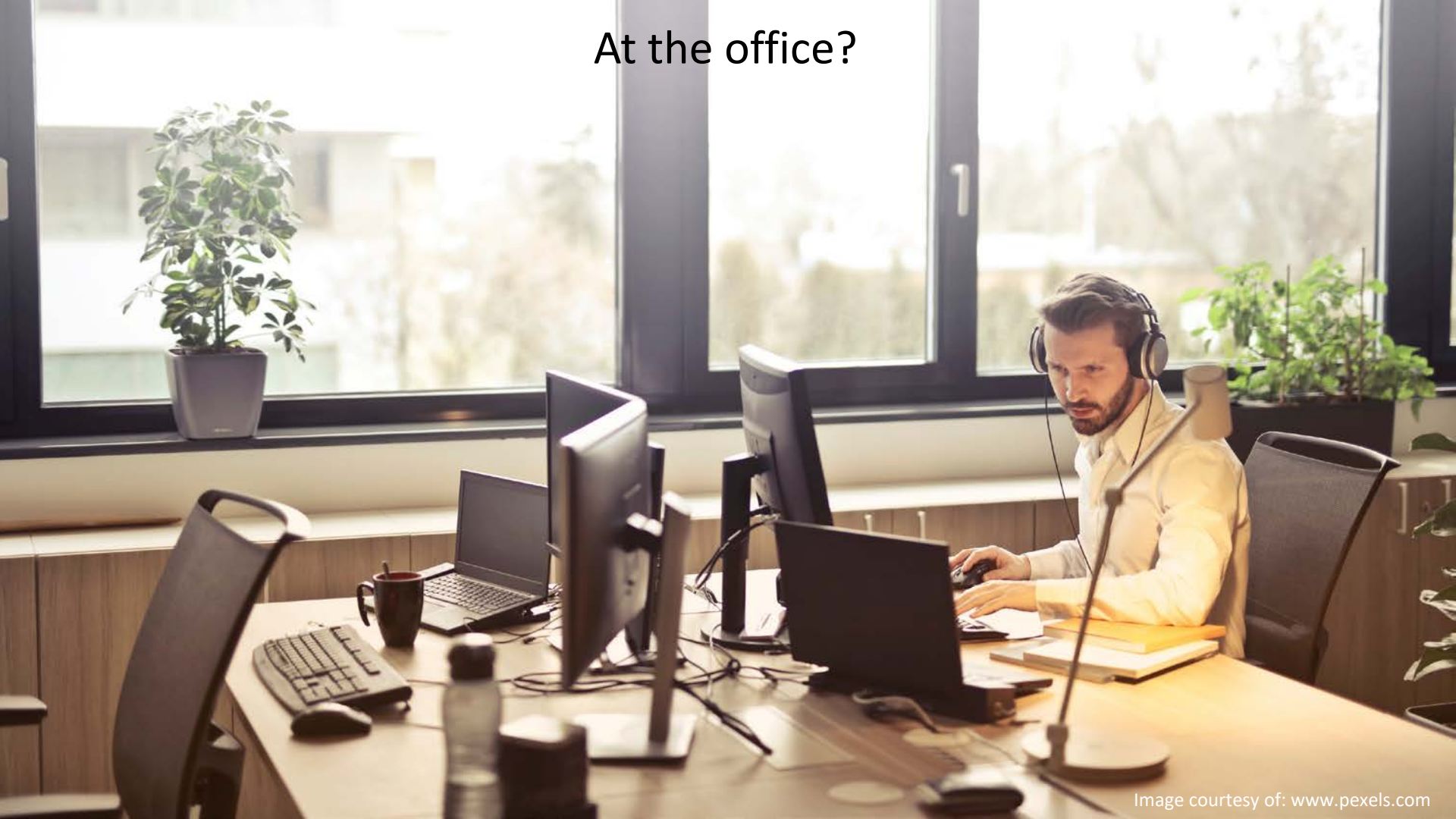


Image courtesy of: www.pexels.com

In the shower?

Photo courtesy of: www.amazon.com

Driving?

Image courtesy of: www.pexels.com

But, what if you were trying to do this?

Image courtesy of: www.pexels.com


Or this?
경 • 찰
Image courtesy of: www.pexels.com

Or this?

Image courtesy of: Instagram - PCarsenault


I mean,
THIS!

Suddenly, this doesn’t seem so complicated.

Image courtesy of: www.pexels.com

What we really want,
is these folks…

Image courtesy of: Flickr artist Thomas Hawke

…doing more of this…

Filmland: Karl Urban in Dredd 3D

…or this…

Image courtesy of: www.pexels.com


??
…and less of this.
???
??!

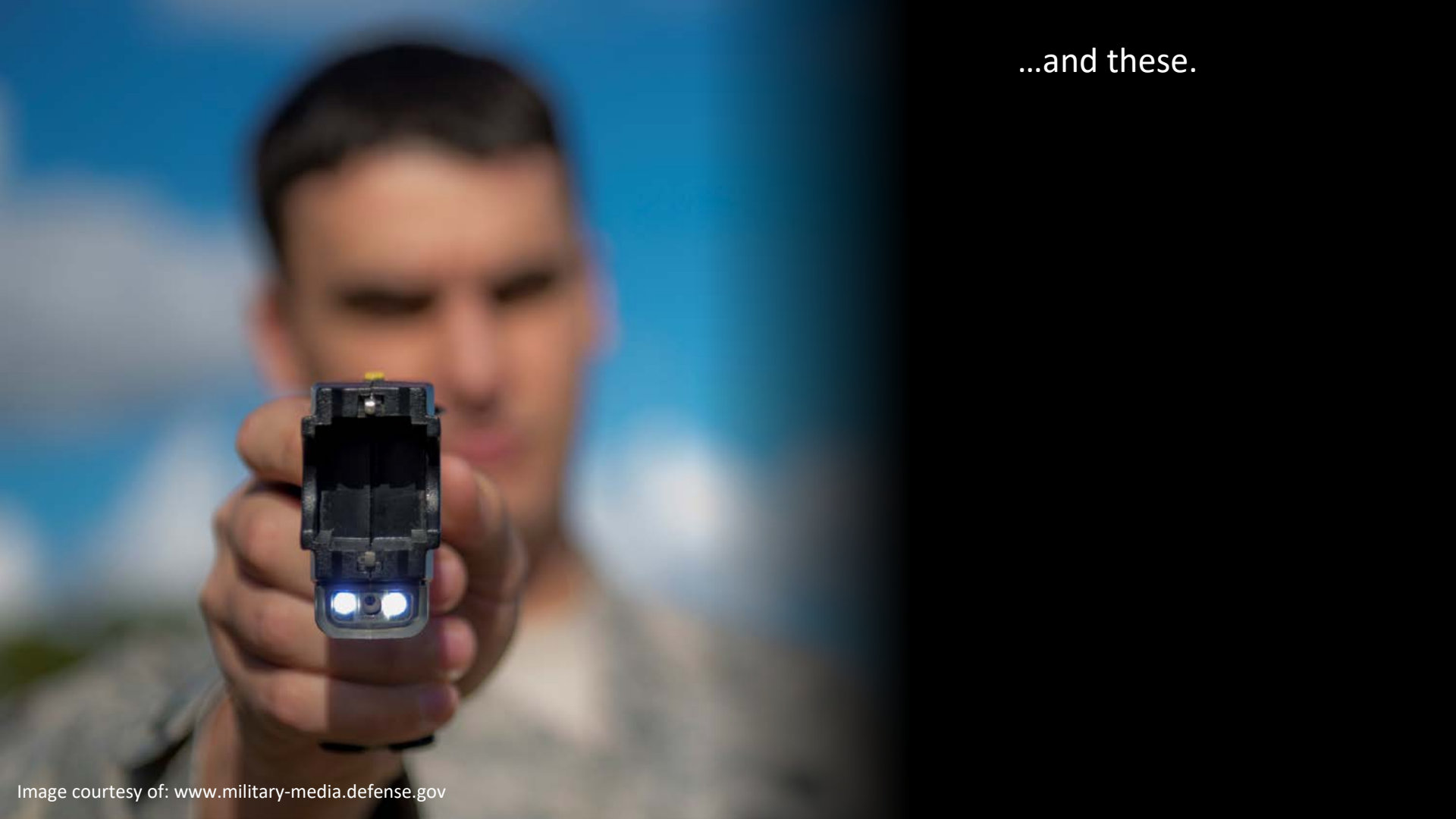
but wait… we'll need to account for these,

Image courtesy of: USAF-E

…and these,

Image courtesy of: www.media.defense.gov

Image courtesy of: www.spoonuniversity.com



…and these.

Image courtesy of: www.military-media.defense.gov

Image courtesy of: www.pexels.com

AND we need to communicate with these,

AND we need to communicate with these,

and these,

AND we need to communicate with these,

and these,

and all of these,

Requirements:

- Authentication that is:
  - Flexible – can handle diverse sets of public safety operational environments
  - Efficient – can be done quickly during line of duty
  - Interoperable – promotes cross-jurisdictional informational sharing

But also…


"Yeaaa, if you could just go ahead and audit all of our user accounts by Monday that would be greaaaaat…"
Office Space © Fox

Requirements:

- Authentication that is:
  - Flexible – can handle diverse sets of public safety operational environments
  - Efficient – can be done quickly during line of duty
  - Interoperable – promotes cross-jurisdictional informational sharing
- Improve credential and account management:
  - Mainly by reducing the number of credentials and accounts needed


And finally…
Definitely want to use AES25…hey bitcoin is over 9000!

Requirements:

- Authentication that is:
  - Flexible – can handle diverse sets of public safety operational environments
  - Efficient – can be done quickly during line of duty
  - Interoperable – promotes cross-jurisdictional informational sharing
- Improve credential and account management:
  - Mainly by reducing the number of credentials and accounts needed
- Get mobile application developers out of:
  - Developing custom authentication solutions
  - Managing users accounts and directory services

Save the world!

Image courtesy of: www.pexels.com


NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE
Accelerate adoption of secure technologies:
collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

NIST Public Safety Communication Research Lab (PSCR) is the primary federal laboratory conducting research, development, testing, and evaluation for public safety communications technologies

WHAT WE BUILT?

Using standards of course!

NCCoE Benefits – Standards-Based

NCCoE solutions implement standards and best practices:

Using modern commercially available technology:

Core Capabilities

Multifactor Authentication (MFA) to Mobile Resources

- Biometrics, external hardware authenticators and other authentication options

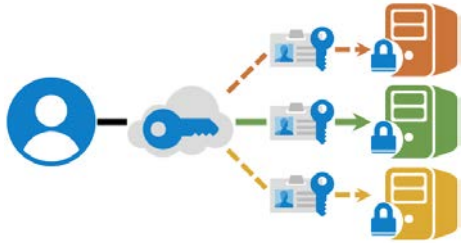
p@$$w0rd +

Single Sign-on (SSO) to Mobile Resources

- Authenticate once with mobile native app or web apps
- Leverage initial MFA when accessing multiple applications

Identity Federation

- Leverage directory services already in place
- Send identities across jurisdictional boundaries



AUTHENTICATION & SINGLE SIGN-ON DEMO

“don’t tell me, show me!”

Demo – What you'll see, MFA + SSO

FIDO UAF Authentication

- Leverages fingerprint registered to device
- No Password Input

Private Key

+

Biometric

FIDO U2F Authentication

- Using FIDO key as second factor
- Private key pair on the device

p1n +

Mobile App Single Sign-On

- Access to mapping and chat apps without need to re-authenticate
- Implements IETF RFC 8252 for SSO on Native Mobile Apps

Demo – What you'll won't see, federation

Identity Federation

- We have examples identity federation using both SAML 2.0 and OpenID Connection 1.0
- But as with all federation its "under the hood"

SOLUTION BENEFITS

“is This Good for the COMPANY?”

Remember password management challenge?

Reduces:

- The amount of authentication time and attempts for PSFR personnel
- The number of credentials that PSFR personnel and organizations need to manage
- Requirements for complex passwords

Standards help!

Increases:

- Interoperability through the use of open, standards-based architecture
  - Identity providers can leverage their current active directory

- Authenticator flexibility through the FIDO ecosystem
  - External hardware authenticators, biometrics, etc…

Standards based MFA

FIDO:

- Multifactor authentication in line with NIST 800-63-3 Requirements
- No secrets (private keys or biometric templates) are stored server-side
  - “verifier compromise resistance”
- Phishing resistance

IETF BCP for Mobile SSO:

- User's password and other credentials are never exposed to the SaaS provider or mobile app
- Apps get an OAuth Token with limited scope of authorization - apps only get access to back-end systems they should be accessing
- Reduced number of credentials decreased risk of credential re-use

Oh by the way… its easy for developers

AppAuth Software Development Kit

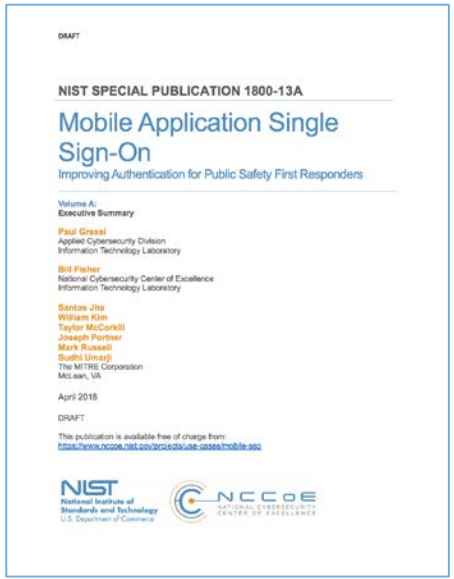
- Implementation of the “OAuth 2.0 for Native Apps” RFC
- Free and open source on GitHub – developed by Google and given to OpenID
- Developers can “Drag and Drop” into a mobile app

NEW NIST GUIDANCE!

“yes but how?”

NIST SP 1800-13 out now for public comment!

- NIST Cybersecurity Practice Guide SP 1800-13 includes:



DRAFT

NIST SPECIAL PUBLICATION 1800-13A

Mobile Application Single Sign-On

Improving Authentication for Public Safety First Responders

Volume A:
Executive Summary

Paul Grassi
Applied Cybersecurity Division
Information Technology Laboratory

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Santos Jha
William Kim
Taylor McCorkill
Joseph Portner
Mark Russell
Sudhi Umarji
The MITRE Corporation
McLean, VA

April 2018

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/use-cases/mobile-sso

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- Technical Decisions
- Trade-offs
- Lessons Learned
- Build Instructions
- Functional Tests

Take-aways?

- 1. Everyone, download SP 1800 -13, Available Now!
- 2. Developers, implement standards-based SSO with AppAuth!
- 3. Check out the FIDO vendors on the RSA exhibit floor

References

- SP 1800-13: https://www.nccoe.nist.gov/projects/use-cases/mobile-sso
- IETF RFC 8252: https://tools.ietf.org/html/rfc8252
- AppAuth: https://github.com/openid/AppAuth-Android
- FIDO: https://fidoalliance.org/about/what-is-fido/

Any questions?

William Fisher, Security Engineer

Email: William.Fisher@nist.gov

Project Updates: https://nccoe.nist.gov/projects/use-cases/mobile-sso