RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART1-R03**

Is Your Passwordless Really Passwordless? How to Tell and Why It Matters

Tim Callan

Chief Compliance Officer
Sectigo

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

“Passwordless” Is a Hot Term

- All kinds of vendor claim to enable “passwordless” authentication
  - They mostly provide some of the benefits of passwordless, but many don’t provide all
- In this session we will cover:
  - Definition of “passwordless”
  - Benefits of true passwordless
  - Technologies that are “pseudo-passwordless”

Why Passwordless Is a Hot Topic Today

- Passwords have serious weaknesses
  - Security
  - User experience
  - Support
- MFA has a similar set of problems
- COVID has been a major forcing function

Benefits of Passwordless

- Better user experience
  - No forgetting passwords
  - No weak/reused passwords
  - Improved employee efficiency
- Reduced support burden
- Better security
  - Eliminates a whole list of password-based attacks

Phishing
Credential stuffing
Brute force attacks
Dictionary attacks
Social engineering
MITM

Passwordless Is Not a User Experience

- The user experience is a by-product of passwordless authentication
  - A password can be present even if the user doesn't know it
- A better user experience is a benefit but not the only benefit
- Passwordless is an architecture

True Passwordless Has No Shared Secret

- A shared secret is not passed across the network
  - Buried passwords are still passwords
  - Password wallets still use passwords
  - Password abstraction layers still use passwords
- In these cases the shared secret is still present, with its vulnerabilities

PINs Are Not Passwords

- A PIN looks like a password but is different in some important ways
  - Ensures the device is in its owner's hands
  - Does not travel across the open internet
- A second factor can share these properties of a PIN
  - e.g. biometric checks

True Passwordless Architecture Is PKI-based

- Asymmetric secrets prevent the many problems of passwords
- Certificates are secure, reliable, and well proven
  - Cryptographically secure beyond possible attack
  - Ubiquitous support across software, hardware, and services
  - A broad variety of options to meet all use cases
- Strong automation alternatives are available
  - Certificate Lifecycle Management
  - ACME
  - And more

Legacy Systems May Not Support True Passwordless

- Older systems with shared-secret credentials as a hard-coded authentication method
- These often mix with newer systems
- Look for closest-possible solutions
  - Implement passwordless where possible and live with passwords where you have no choice
  - Look at SSO or other options to lessen the pain for these old systems
  - When updates do occur, look to add passwordless
  - Don’t fall for the lowest common denominator fallacy

How to Apply

- Understand the security differences between passwordless and pseudo-passwordless
  - Pseudo-passwordless may still have benefits, but we must be clear on what we are getting
- Clarify these differences to stakeholders
- Consider phased-in and hybrid approaches to deal with pragmatic realities
  - For some use cases pseudo-passwordless may prove good enough, while others may require true passwordless

If you liked this conversation…

ROOT CAUSES

A PKI & Security Podcast

Available on these streaming services

iTunes

Spotify

SOUNDCLOUD

STITCHER

iHeartRADIO

…and others

RSAConference2022

Questions