Passwords?
To Infinity and Beyond!

Glennon Bagsby & Julie-Ann Williams
NewEra Software Inc. & millennia…

November 2018
Session FB




Agenda

- Who Are We?
  - Glennon Bagsby
  - Julie-Ann Williams
- What is “User Authentication”?
  - Basic and Advanced
- The Past…
- The Present…
- The Future…
- To Infinity and Beyond!

- Thank you ☺

Who are we?

- Glennon Bagsby
  - President at NewEra Software Inc.
  - 46 years
    - Systems Software specialist – z/OS
    - Special interest in operating system integrity

Who are we?

- Julie-Ann Williams
  - Mainframe Evangelist at millennia…
  - 35 years
    - Operating System Specialist – z/OS
    - Mainframe Architect
    - Security Specialist – including CA ACF2, CA Top Secret and IBM RACF

millennia…

What is “User Authentication”?

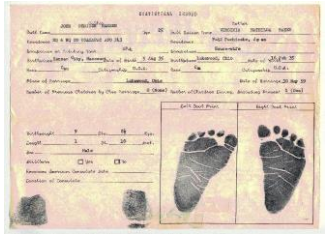
- Basic
  - How we confirm who is signing on to the system and when
    - e.g. Userid **AND** Password
  - Distinct from “User Authorisation”

- Advanced - Wikipedia
  - Authentication (from Greek: αὐθεντικός authentikos, "real, genuine", from αὐθέντης authentes, "author") is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. In contrast with identification, which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the authenticity of a website with a digital certificate, determining the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

What is “User Authentication”?

- Not a problem that is unique to IT
  - Passports
  - Finger Prints
  - Birth Certificates
  - Electronic Gadgets
    - Multi Factor
  - etc
- No current solution to all the known problems!
- Which doesn’t mean it’s appropriate NOT to check!

etc…



The Past…

- In the beginning these were called “computers”

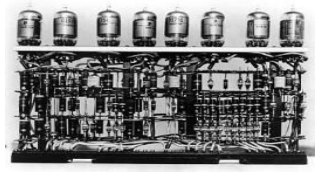
!

The “brain” [computer] may one day come down to our level [of the common people] and help with our income-tax and book-keeping calculations. But this is speculation and there is no sign of it so far.

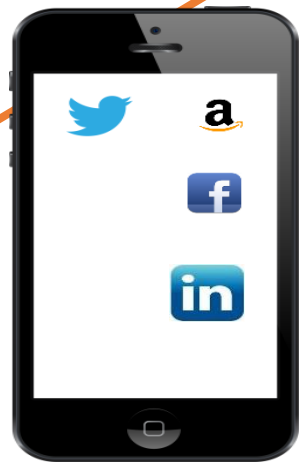
The Star - June 1949

The Past…

- Then the 1950s happened!



Barry Schrager wrote the first paper on computer security for SHARE before producing ACF2!



1972

2018

1950s

- We now live in a Sci Fi Future World!

The Present…

- Security can’t win in the battle with Usability
- More or less standardised use of Userid and password to authenticate mainframe users
  - Mainframe Passwords:
    - 8 characters
    - Mixed case
    - Some special characters
    - Do not normally qualify as “strong passwords”
  - Mainframe Pass Phrases:
    - COULD resolve problems of password “strength”
    - In reality… Not being used ☹
  - Mainframe Digital Certificates…

The Present…

- Available options (without judgement on strength/appropriateness)
  - Single Signon
    - Dying out due to limitations
  - Session Managers
    - Can help with managing multiple ids from a single platform
  - Password Vaults
    - e.g. McAfee True Key
  - Multi Factor Authentication
    - Commonly deployed to an increasing global audience
    - OTPs (One Time Password)
  - Biometrics
    - The picture of how advance biometrics really is has been thoroughly skewed by the number of mobile device users relying heavily on finger print scanners/facial recognition.

The Present…

- The future of Mainframe Passwords is here today on non Mainframe platforms.

amazon

To verify your identity, please use the following code:
133441
Amazon takes your account security very seriously. Amazon will never email you and ask you to disclose or verify your Amazon password, credit card, or banking account number. If you receive a suspicious email with a link to update your account information, do not click on the link—instead, report the email to Amazon for investigation.
We hope to see you again soon.

Microsoft account
Your password changed
Your password for the Microsoft account
gh*****@newera.com was changed on 11/3/2018 4:33 PM (CST).

If this was you, then you can safely ignore this email.

Security info used: ghb@newera.comCountry/region: United States
Platform: WindowsBrowser: Microsoft EdgeIP
address: 66.254.206.13

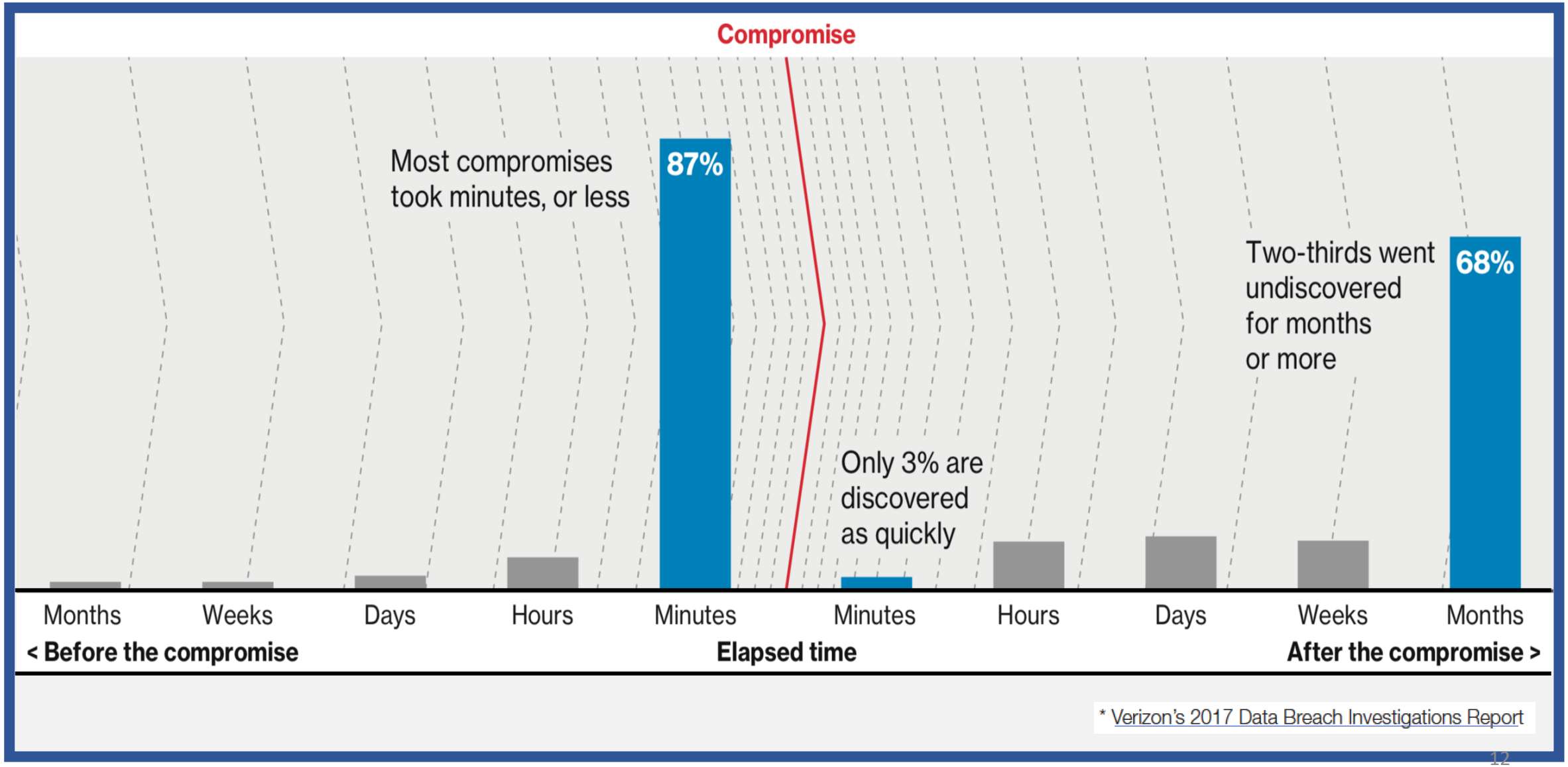
If this wasn't you, your account has been compromised.
Please follow these steps:
1. Reset your password.
2. 2. Review your security info.
3. 3. Learn how to make your account more secure.

You can also opt out or change where you receive security notifications.

Thanks,
The Microsoft account team

Remember: The only person who knows what you're doing at any point in time is you!

The Integrity Controls Environment – Defend against and Detect the Intruder!



* Verizon's 2017 Data Breach Investigations Report

MONITOR USER LOGONS

- With notification sent to User and/or Others

```
01C|-SRC: LOGONRST-------------THE CONTROL EDITOR--------------- OTPNotify -

02C|SYSPLX:ADCDPL   SYSNM:ADCD22B  USRID:GBAGS2      TM:11:09:49 DT:04/18/18

03C|-OTPNOTIFY: GBAGS2-----------------------------------------------------

-----------------------------------EVENT DATA-----------------------------------

To complete the reset request, logon to the system of record prior

to 11:15:26 system time using OTP new value jC9T7po3
```

MONITOR USER LOGONS

- With notification sent to User and/or Others

```
01C|-SRC: LOGON----------------THE CONTROL EDITOR------------------ Notify -

02C|SYSPLX:ADCDPL   SYSNM:ADCD22B  USRID:GBAGS1      TM:11:08:36 DT:04/18/18

03C|-PSWDCHNG: GBAGS1-----------------------------------------------------
```

MONITOR USER LOGONS

- With notification sent to User and/or Others

```
01C|-SRC: SYSLOGON(Unknown )---THE CONTROL EDITOR---------- VerifyFail -

02C|SYSPLX:ADCDPL   SYSNM:ADCD22B  USRID:GBAGS2      TM:07:39:39 DT:04/13/18

03C|-VERIFY(X): GBAGS2----RC: 08 Password or phrase is not authorized


01C|-SRC: SYSLOGON(TOKTSO  )---THE CONTROL EDITOR------ VerifySuccess -

02C|SYSPLX:ADCDPL   SYSNM:ADCD22B  USRID:********    TM:10:45:36 DT:04/17/18

03C|-VERIFY(X): KINGSTON-------------------------RC: 00--------------------
```

MONITOR USER LOGONS

- With notification sent to User and/or Others

```
01C|-SRC: SYSLOGON(TOKTSO  )---THE CONTROL EDITOR-------------- VerifyFail -

02C|SYSPLX:ADCDPL   SYSNM:ADCD22B  USRID:PROBO1      TM:17:21:37 DT:04/18/18

03C|-VERIFY(X): PROBO1----RC: 04 User profile not defined to RACF ----------
```

The Present…

- Password Evolution
  - Increase password strength
  - Blockers on mainframe?
    - Only substandard passwords?
    - Only 8 characters?
    - Mixed case/Special Characters?
    - Other “excuses”?

Homeland Security

US-CERT United States Computer Emergency Readiness Team

National Cyber Awareness System:

TA18-276A: Using Rigorous Credential Control to Mitigate Trusted Network Exploitation

10/03/2018 07:00 AM EDT

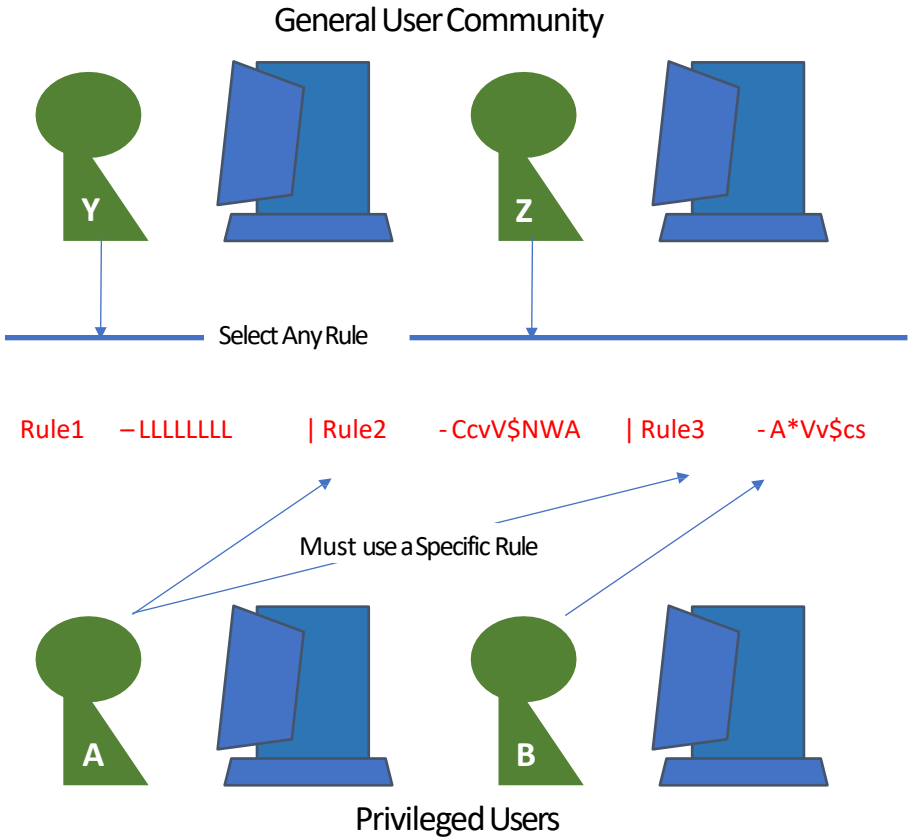
Original release date: October 03, 2018

“Compromising the credentials of legitimate users automatically provides a threat actor access to the network resources available to those users and helps that threat actor move more covertly through the network. Adopting and enforcing a strong-password policy can reduce a threat actor’s ability to compromise legitimate accounts; transitioning to multifactor authentication solutions increases the difficulty even further. Additionally, monitoring user account logins— whether failed or successful—and deploying tools and services to detect illicit use of credentials can help network defenders identify potentially malicious activity.”

Remember: The only person who knows what you’re doing at any point in time is you!

The Present…

- Password Format Binding…
  - IBM Security Server RACF provides for eight syntax format rules. These rules can vary considerably in terms of complexity. Users can choose which available rule they will conform to during password/passphrase reset process.
  - Some users may select a complex rule, but others might succumb to 'Human Nature' and select the simplest; perhaps because it's easier to remember.
  - This flexibility makes it difficult to implement a requirement for more complexity as doing so would impact the entire user community.
  - Format binding overcomes this "Catch 22" by allowing your security team to assign more complex formats on a user by user basis to privileged users, while allowing general users to select formats as they have been trained.



Remember: The only person who knows what you're doing at any point in time is you!

The Present…

- Multi Factor Authentication
  - More commonly used (Online banking usually deploys MFA).
  - Users more willing to accept the technology.
  - Adds security without removing too much usability.
  - A number of mainframe implementations:
    - IBM
    - New Era Software Inc.
    - Vanguard
    - etc

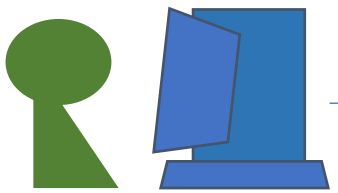
- One Time Passwords (OTP)
  - Moving away from SMS delivery towards encrypted delivery mechanisms.

Remember: The only person who knows what you're doing at any point in time is you!

The Present…

- Multi-Factor Reset (MFR) & Multi-Factor Logon (MFL)
  - *A four 'Factor', 100% software solution for implementing so called MFA on IBM z/OS Systems*
  - *Validity Window: 1, 2, 4, 8, 12, 24 Hours*
  - *Prefix (4/6 characters) and Suffix (4/8 characters) are ch*
    manner that is asynchronous to each other.
  - *Users register/request the Prefix, the System build*
  - *The combination is required for logon during th*
  - *When the Window terminates, the process be*
  - *The user never knows the full Password/Phrase in adva*

Demo Time!



Privileged

Registered Password Prefix
(Registered at any time)

UserId + Password/Phrase

UserId + Prefix||Suffix

Interval Password Suffix
(Generated in Real Time)

When a Password is used to Logon
PFIX012S or PFIXo12S
When a Passphrase is used to Logon
PREFIXJKLMO12S or PREFIXjKlmo12S

IBM RACF

CA/ACF2

CA/Top Secret

z/OS

Remember: The only person who knows what you're doing at any point in time is you!

What happens if MFA Fails ?

- With notification sent to User and/or Others

```
01C|-SRC: EXPCHECK-------------THE CONTROL EDITOR------------ ExpiryNotify -
02C|SYSPLX:ADCDPL   SYSNM:ADCD22B  USRID:********    TM:00:15:00 DT:09/16/18
03C|-PSWDEXP: EXPIRATION CHECKER FOR RFAUL2-----Password expires in 29 days-
```

The Future…

- Passwordless access!
  - Strong, frictionless biometrics?
  - Geospatial awareness?
  - ???

- Forbes Technology Council…

"While all of these authentication methods work to safely confirm that all transactions are legitimate, no single technology will secure online financial transactions with 100% certainty. The key is to stay one step ahead of cybercriminals while preserving a low-friction customer experience. Passwords do neither of those. It's time to step up and embrace the latest in what strong multifactor authentication has to offer."

To Infinity and Beyond!

- **If even Facebook can do it…**
  - USER becomes part of the Security Paradigm!
  - If access is used and it is not the authorised user they can contact:
    - Sec Admin to have ID revoked and/or cancelled
    - Audit notified and any actions flagged
  - Notifications issued real time:
    - can be sent to:
      - Users
      - Administrators
      - Audit
      - Anyone/thing you choose!
  - Successful **AND** unsuccessful logon events should be notified


Facebook

Hi xxxxxxxx,

Your Facebook password was changed on Friday, 17 November 2017 at 19:34 (UTC).

Operating system: Windows
Browser: Chrome
IP address:
Estimated location: Somewhere, ENGLAND, GB

If you did this, you can safely disregard this email.

If you didn't do this, please secure your account.

Thanks,
The Facebook Security Team

This message was sent to someone@xxxxxxxxx.com. If you don't want to receive these emails from Facebook in the future, please unsubscribe.
Facebook, Inc., Attention: Community Support, 1 Hacker Way, Menlo Park, CA 94025

- **You can do it too! Don't delay…**

Remember: The only person who knows what you're doing at any point in time is you!

We want your feedback!

- Please submit your feedback online at ….
  - http://conferences.gse.org.uk/2018/feedback/FB

- Paper feedback forms are also available from the Chair person

- This session is FB