Don’t let your mainframe passwords be the weakest link in your enterprise

June 20, 2019

Sponsored by

Carbon Black.

@BlackHatEvents / #BlackHatWebcasts

Speakers

Featured Presenter:

Chad Rikansrud, @bigendiansmalls

Director of North American Operations,

RSM Partners

Sponsor Presenter:

David Balcar, @network232

Security Strategist,

Carbon Black

Sponsored by

Carbon Black.

About Me

- Director RSM Partners
  - All mainframe, all the time
- Global Banking Technology Leader for 20 years
  - Ran global data center operations
  - Responsible for mainframe data protection
- Moving mainframe security forward
  - Penetration Testing (& other mainframe services) – rsmpartners.com
  - Tools – Metasploit, others
  - Training – evilmainframe.com

Intro

- Mainframe
  - IBM z/OS for our purposes today
  - Underpins global economy today
- New, updated, powerful
  - 32 TB RAM, Up to 170 cores
- Very backwards compatible & reliable
- ***Not legacy – The Windows Example***

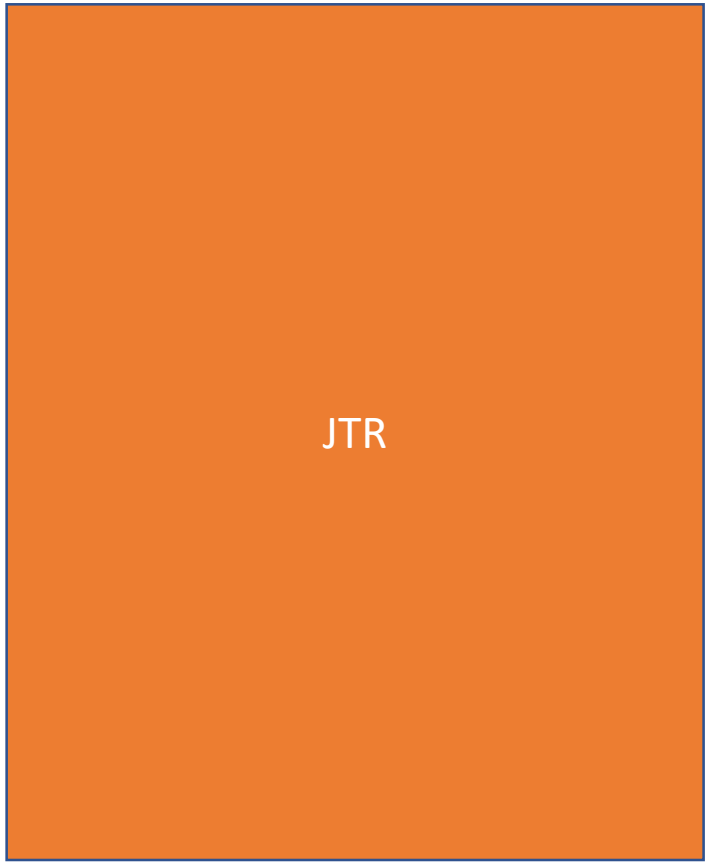
  ”Just because it has its roots in the 60s, doesn’t make it legacy” -Me

Myths

- Your banking app passwords are terrible because of your mainframe
  - Banking webapps are typically their own stand-alone applications
- z/OS (RACF) is limited to upper/digits and 8-character passwords
  - Mixed case and special character support has been around for years
- Mainframes only run COBOL
  - Mainframes run: C/C++, Java, PL/I, COBOL, NodeJS, web-apps and others.
- Mainframes are “legacy” technology that is old and outdated
  - z/OS has a new release every couple years; and the hardware was refreshed last year

Types of RACF Authentication

- Password Algorithms
  - Stores encrypted User ID, not password hash
    - Password->Hash->Key->Encrypted User ID Stored
  - Why limited to 8 characters
  - DES
    - 1970s algorithm, super fast block cipher
  - KDFAES
    - Released in 2014, based on PBKDF2, much much slower (70,000 – 140,000 times depending on equipment and tools)



Types of RACF Authentication (continued)

- Passphrases
  - 14 to 100 characters, been supported for years
  - But! No one uses them because of interfaces which do/may restrict length to 8 characters
  - Long enough makes them near impossible to brute force
- Passtickets
  - Used for app level access to system – so passwords don’t have to be used
  - Similar to a TOTP (Google Authenticator) access
  - Seeds can be stored encrypted in the RACF database (or masked)
  - Time limited (10 minutes default)

Enterprise Password Synchronization

- Why might it be a terrible idea to sync your enterprise (i.e. single sign-on) with your mainframe passwords?
  - Your mainframe password policy may be weaker than your enterprise one
  - Or vice-versa
- Passwords from one or the other could be cracked / reused

This could make MF passwords the ‘weak link’ in the enterprise if you’re single sign-on, e.g. steal racf db, crack all the passwords, pwn DA

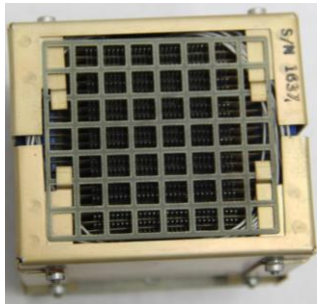
Key Takeaways

- Always use random bytes for passticket seeds and use strong encryption (versus masking) to store in the RACF database
- Both RACF algorithms (DES and KDFAES) support multi-factor authentication (MFA)
- Don’t overlook passphrases, it might not be as hard as you think
- Use KDFAES to make offline brute-forcing more difficult
- Don’t synchronize with your enterprise passwords unless you are using MFA or passphrases (or both!)

Been There Done That!

AN/UYK-20 computer

Core memory



Sperry/UNIVAC

Dave's Top 5

5. Know your network & Log everything
4. Train your Security staff
3. MFA for everyone
2. Password Managers are not the evil twin
1. Long passwords/passphrases are da bomb…

Questions & Answers

Featured Presenter:

Chad Rikansrud, @bigendiansmalls

Director of North American Operations,

RSM Partners

Sponsor Presenter:

David Balcar, @network232

Security Strategist,

Carbon Black

- **To join the Black Hat mailing list, email BH LIST to:** feedback@blackhat.com
- **To join our LinkedIn Group:** http://www.linkedin.com/groups?gid=37658&trk=hb_side_g
- **To follow Black Hat on Twitter:** https://twitter.com/Blackhatevents
- **Black Hat's Facebook Fan Page:** http://www.facebook.com/blackhat
- **Find out more at www.blackhat.com**
- **Next Webcast: July 18, 2019**

Sponsored by

Carbon Black.

Thank You!