

Mainframe passwords revisited: impact of new security mechanisms

Costin Enache, Chad Rikansrud, Nigel Pentland

GSE UK Security Working Group – 4th February 2021

This slide deck: ~20 minutes

Panel discussion and Q&A: ~40 minutes

Who are we?

- Chad Rikansrud

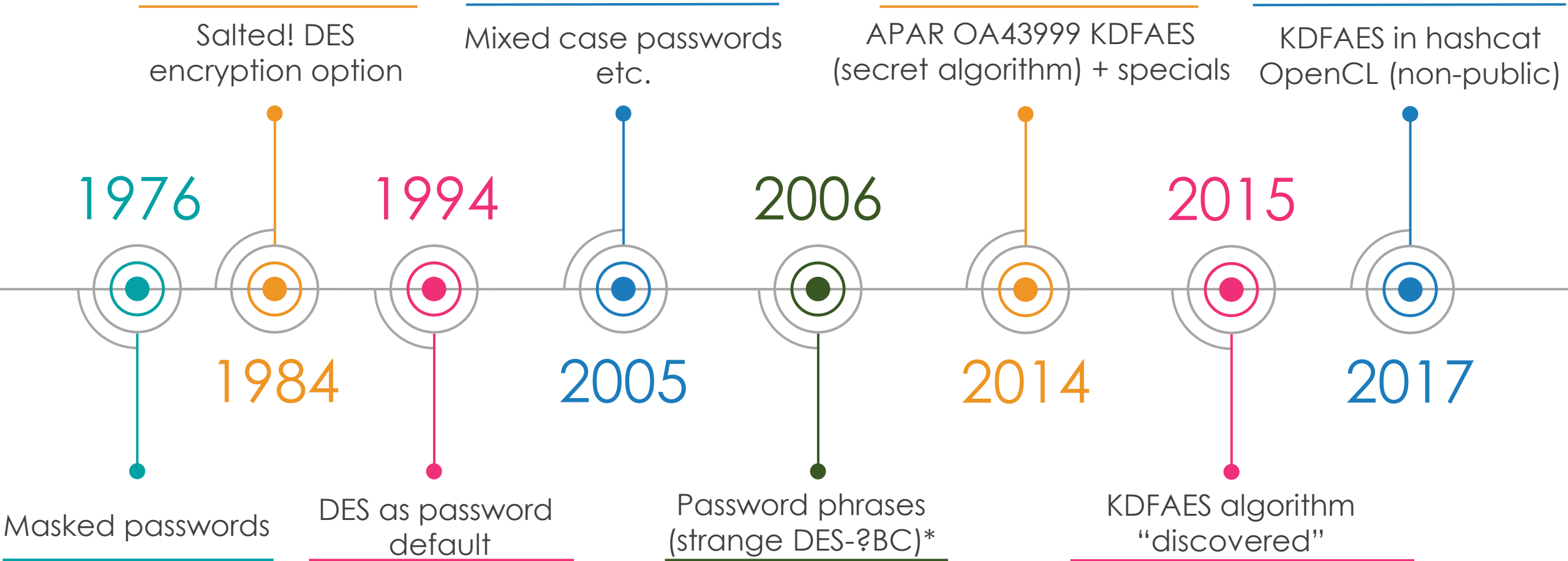
IT security consultant, Director of North American Consulting Services for BMC, performing mainframe security assessments, exploit development, and penetration tests for some of the world's largest organizations for 20+ years. chad_rikansrud@bmc.com

- Nigel Pentland

Senior Security Analyst at NAB, retired. The authority on mainframe passwords for many years and the author of the original analytics tools that saved many of us. nigel@nigelpentland.net

- Costin Enache

IT security consultant and occasional developer, MD at Detack.de, been working with mainframe security for 20+ years; author of EPAS, a toolset for password analytics that includes RACF with KDFAES support. costin@detack.de



*IBMUSER:AGoodPassword2001 = AGoodPassword2002 = 1D80A5E7A1C14709DD0C44377CBD8303E0

The KDFAES Algorithm

- **Step #1:** Calculate input for key derivation, K_i

Passwords: $K_i[8] = \text{Old DES password} = \text{DES}(K=\text{password}, \text{In}=\text{username})$; permits **one-way migration** of old DES

Password phrases: $K_i[40] = \text{SHA256}(\text{phrase}) + \text{length}(\text{phrase})$; no migration possible for DES phrases

- **Step #2:** Key derivation based on custom IBM version of PBKDF2-SHA256; 45008 rounds*

$K_d = \text{IBM-PBKDF2-SHA256}(\text{RANDOM_SALT}[16], K_i, 45008)$

- **Step #3:** Encrypt, by using AES256, the user name with the derived key

$\text{Hash}[32] = \text{AES256}(K=K_d, \text{In}=\text{username}) + \text{RANDOM_SALT}[16]$

- **The icing on the cake:** It is quantum-safe 😊 Both SHA256 and AES256 are believed to be safe.

*The algorithm includes 2 parameters (**memory and repetition factors**) which can be customized and get stored within the hash. This allows the key derivation step to be future-proof, i.e., get slower. Not in use for now, but if maxed out, the computation time is increased ~4500 times

Link: https://github.com/openwall/john/blob/bleeding-jumbo/src/racf_kdfaes_fmt_plug.c

The Tools: Cluster, Big Server, Amazon EC2

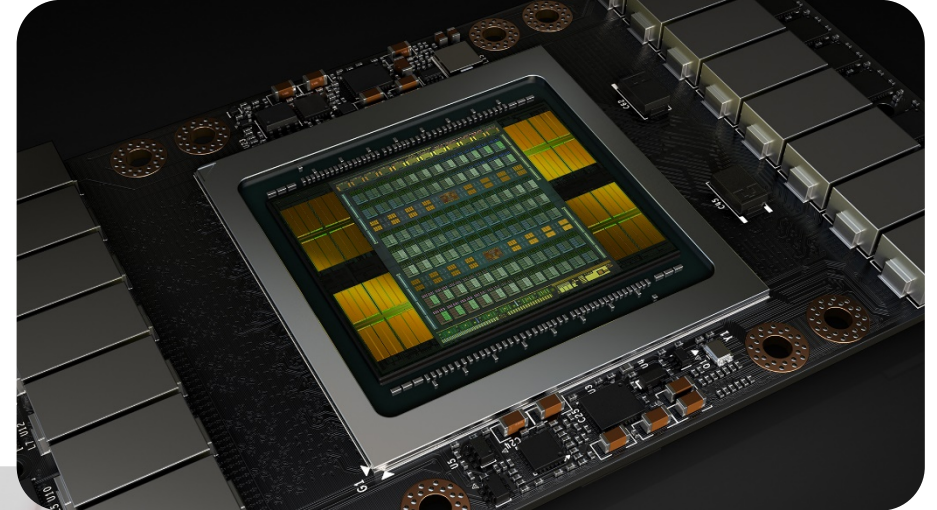


- 6 x GPU Worker Cluster

Examples based on 1xGPU



- 10 x GPU Worker, Single Unit



- 1 x Amazon EC2 p3.16xlarge

DES Performance: Brute Force

The screenshot shows the 'epas Jobs - View Audit Log' interface. The left sidebar contains navigation links: Dashboard, Targets, Audit Jobs (selected), Jobs List, New Job, Audit Profiles, New Audit Profile, Settings, Analyser, Enforcer, Reports, System, and Logout. The main content area has tabs for Main, Job Log (selected), Job History, and Return to List. Under 'Job Actions', there are buttons: Run Now, Stop Running Job, Interrupt Step, Suspend Job, Resume Job, Clone Job, Clear History, and Delete. The 'Master Log' section shows a series of status messages from 01/31/2021 02:50:05 to 02:50:06, including password hashes retrieved, preliminary mode preparation, initial/default passwords, known information words, empty site information, dictionary mode preparation, dictionary mode words, brute force mode preparation, and starting all worker processes. The 'Worker Log' section shows real-time data for worker W001, including passwords per second (7912.4 MH/S), time spent (1 minute, 5 seconds), time left (10 minutes, 14 seconds), key space searched (9.14%), status (RUNNING), recovered hashes (99), valid hashes left (1), and cumulative time (2 minutes, 1 second). A 'Refresh' button is at the bottom.

DES: Brute Force Probing

Upper Case

Standard Character Set

8-Character Password

Users: 1

Guaranteed Recovery: 13 min

Worker: 1 x Nvidia 3090 GPU

KDFAES Performance: Brute Force

epas Jobs - View Audit Log

https://epas-lab.detack.de/job.php?action=log&id=4

Dashboard

Targets

Audit Jobs

Jobs List

New Job

Audit Profiles

New Audit Profile

Settings

Analysers

Enforcer

Reports

System

Logout

2021-01-31 06:00 CET

© 2011-2020 Praetors AG 1.0.38

Main Job Log Return to List

Job Actions

Run Now Stop Running Job Interrupt Step Suspend Job Resume Job Clone Job Clear History Delete

Master Log

```

=== 01/31/2021 03:01:29 Password hashes retrieved: 100
=== 01/31/2021 03:01:29 Preparing preliminary mode
=== 01/31/2021 03:01:29 Initial/default passwords: 28
=== 01/31/2021 03:01:29 Known information words: 734
=== 01/31/2021 03:01:29 Empty site information, using default data
=== 01/31/2021 03:01:29 Preparing dictionary mode
=== 01/31/2021 03:01:29 Dictionary mode words: 35136034
=== 01/31/2021 03:01:29 Preparing brute force mode
=== 01/31/2021 03:01:30 Started all worker processes
    
```

Worker Log

```

W001 === CURRENT STEP REALTIME DATA REQUESTED AT SUN JAN 31 06:00:13 CET 2021 ===
W001 PASSWORDS/SECOND: 72176 H/S
W001 TIME SPENT/STEP: 13 SECONDS (LENGTH=8)
W001 TIME LEFT: 858 DAYS, 5 HOURS
W001 KEYSPEC SEARCHED: 0.00%
W001 STATUS: RUNNING
W001 RECOVERED HASHES: 99
W001 VALID HASHES LEFT: 1
W001 CUMULATIVE TIME: 2 HOURS, 58 MINUTES
W001 === REALTIME DATA FOR CURRENT STEP END ===
    
```

Refresh

KDFDES: Brute Force Probing

Upper Case

Standard Character Set

8-Character Password

Users: 1

Guaranteed Recovery: 858 days

Worker: 1 x Nvidia 3090 GPU

```

root@epas61:/epas/processors/jtr# ./jtr-avx-normal --test --format=epas-racf-pwk-nocase
will run 32 OpenMP threads
Benchmarking: epas-racf-pwk-nocase, EPAS RACF PW KDFAES NOCASE V0.1 [DES-PBKDF2-SHA256-AES 128/128 AVX 4x]... (32xOMP)
Warning: "Many salts" test limited: 2/256
Many salts: 1131 c/s real, 35.6 c/s virtual
Only one salt: 1119 c/s real, 35.6 c/s virtual
    
```

DES Performance: Wordlist

The screenshot shows the 'epas Jobs - View Audit Log History' interface. The browser address bar displays 'https://epas-lab.detack.de/job.php?action=hist&id=2&hist=1'. The left sidebar contains navigation links: Dashboard, Targets, Audit Jobs (selected), Jobs List, New Job, Audit Profiles, New Audit Profile, Settings, Analyser, Enforcer, Reports, System, and Logout. The main content area has tabs for Main, Job Log, Job History (selected), and Return to List. Under 'Job Actions', there are buttons: Run Now, Stop Running Job, Interrupt Step, Suspend Job, Resume Job, Clone Job, Clear History, and Delete. The 'Master Log' section shows a timeline of events from 01/31/2021 02:50:06 to 02:55:13, including starting worker processes, job data collection, report generation, and processing of dictionary and group membership content. The 'Worker Log' section shows detailed performance metrics for worker W001, including password hashes tested (100), dictionary mode (STARTING STRAIGHT DICTIONARY STEP), time limit (05:00:00), current step passwords per second (452.3 MH/S), current step time spent (5 SECONDS), current step key space searched (100.00%), current step ended with status (COMPLETE), current step hashes left (1), and cumulative time spent (34 SECONDS). A green box highlights the 'CURRENT STEP' details. At the bottom, there is a 'Return to History' button and a status bar showing '2021-01-31 04:00 CET' and '© 2011-2020 Praetors AG 1.0.38'.

DES: Wordlist Probing

Upper Case

Standard Character Set

8-Character Password

Users: 100

Dictionary: 35,136,034

Complete Keyspace: 5 seconds

Worker: 1 x Nvidia 3090 GPU

KDFAES Performance: Wordlist

The screenshot shows the 'epas Jobs - View Audit Log' interface. The left sidebar contains navigation links: Dashboard, Targets, Audit Jobs (selected), Jobs List, New Job, Audit Profiles, New Audit Profile, Settings, Analyser, Enforcer, Reports, System, and Logout. The main content area has tabs for Main, Job Log, and Return to List. Under the Job Log tab, there are buttons for Run Now, Stop Running Job, Interrupt Step, Suspend Job, Resume Job, Clone Job, Clear History, and Delete. The Master Log section displays a list of job actions with timestamps. The Worker Log section shows detailed performance metrics for a specific worker (W001).

Master Log

```

=== 01/31/2021 03:01:29 Password hashes retrieved: 100
=== 01/31/2021 03:01:29 Preparing preliminary mode
=== 01/31/2021 03:01:29 Initial/default passwords: 28
=== 01/31/2021 03:01:29 Known information words: 734
=== 01/31/2021 03:01:29 Empty site information, using default data
=== 01/31/2021 03:01:29 Preparing dictionary mode
=== 01/31/2021 03:01:29 Dictionary mode words: 35136034
=== 01/31/2021 03:01:29 Preparing brute force mode
=== 01/31/2021 03:01:30 Started all worker processes
  
```

Worker Log

```

W001 === CURRENT STEP REALTIME DATA REQUESTED AT SUN JAN 31 05:49:28 CET 2021 ===
W001 PASSWORDS/SECOND: 75251 H/S
W001 TIME SPENT/STEP: 2 HOURS, 44 MINUTES
W001 TIME LEFT: 3 HOURS, 27 MINUTES
W001 KEYSpace SEARCHED: 37.93%
W001 STATUS: RUNNING
W001 RECOVERED HASHES: 40
W001 VALID HASHES LEFT: 60
W001 CUMULATIVE TIME: 2 HOURS, 47 MINUTES
W001 === REALTIME DATA FOR CURRENT STEP END ===
  
```

2021-01-31 05:49 CET i

© 2011-2020 Praetors AG 1.0.38

KDFDES: Wordlist Probing

Upper Case

Standard Character Set

8-Character Password

Users: 100

Dictionary: 35,136,034

Complete Keyspace: 6 hours

Worker: 1 x Nvidia 3090 GPU

Numbers Compared

- 3090 GPU Worker Instance (HW Price: €30k)

	1 x GPU		10 x GPU	
RACF KDFAES	80,449	H/s	800,210	H/s
RACF DES	7,467	MH/s	73,716	MH/s
NTLM	116,602	MH/s	1,149,035	MH/s

- Amazon EC2 p3.16xlarge (HW Price: €20/h)

	1 x GPU		8 x GPU	
RACF KDFAES	71,193	H/s	569,550	H/s
RACF DES	5,809	MH/s	46,564	MH/s
NTLM	102,202	MH/s	818,215	MH/s

- Apparently: Average of **85,000** times harder to crack KDFAES than DES via **brute force** attacks
- And **1,500,000** times harder than NTLM

2010 DES

- 8 Core server system, CPU-only ~ €3000

Off the shelf JtR:

8 x 778,752 = **6,230,016** H/s

Smarter JtR (EPAS: Bitslice DES, AVX/SSE2):

8 x 24,925,141 = **199,401,128** H/s ~aprox. 33x faster

- Between **11** and **2,500** times harder to crack a RACF password in 2020 (KDFAES) compared to 2010 (DES)

2020 KDFAES

- Server with 3090 GPU ~ €3000

OpenCL / CUDA:

80,449 H/s

- Amazon 8xGPU p3.16xlarge for ~ 1 week ~€3000

8 x 71,193 = **569,550** H/s

Are RACF password hashes now safe?

- Brute-force attacks are no longer a viable option
- Current OpenCL hardware and cloud resources still provide a good speed of between 80,000 and 800,000 H/s
- Hash cracking is still possible, but the keypace must be trimmed; attackers were doing this anyway
- Anatomy of a real attack:

Minimize the number of users: target service, privileged, developer, TSO accounts only

Use wordlists customized for the current target: leaked passwords, company branding

- Even better, what we do when we run RACF security assessments:

Target a weaker system first, say Active Directory (unsalted), and use the recovered passwords as wordlist

Many users will have identical or similar passwords; nobody needs to crack all of them, one is usually enough

NTLM: Fast Cracking, No Salt

The screenshot shows the 'epas Jobs - View Audit Log' page in a web browser. The URL is <https://epas-lab.detack.de/job.php?action=log&id=7>. The interface has a dark sidebar with navigation links: Dashboard, Targets, Audit Jobs (selected), Jobs List, New Job, Audit Profiles, New Audit Profile, Settings, Analyser, Enforcer, Reports, System, and Logout. The main content area shows the 'Job Log' for job ID 7. It includes a 'Job Actions' bar with buttons like 'Run Now', 'Stop Running Job', 'Interrupt Step', 'Suspend Job', 'Resume Job', 'Clone Job', 'Clear History', and 'Delete'. Below this is the 'Master Log' showing the initial setup steps, including preparing LM hashes and dictionary mode. The 'Worker Log' section shows real-time data for a worker, including passwords per second, time spent, and cumulative time. A 'Refresh' button is at the bottom of the Worker Log.

Job Actions

Run Now *i* Stop Running Job *i* Interrupt Step *i* Suspend Job *i* Resume Job *i* Clone Job *i* Clear History *i* Delete *i*

Master Log

```

=== 01/31/2021 06:38:57 Initial/default passwords: 47
=== 01/31/2021 06:38:57 Known information words: 40499
=== 01/31/2021 06:38:57 Site information words: 40499
=== 01/31/2021 06:38:57 Preparing LM hashes source mode
=== 01/31/2021 06:38:57 No LM hashes found, skipping this mode
=== 01/31/2021 06:38:57 Preparing dictionary mode
=== 01/31/2021 06:38:57 Dictionary mode words: 35136034
=== 01/31/2021 06:38:57 Preparing brute force mode
=== 01/31/2021 06:38:58 Started all worker processes
    
```

Worker Log

```

W001 === CURRENT STEP REALTIME DATA REQUESTED AT SUN JAN 31 07:04:15 CET 2021 ===
W001 PASSWORDS/SECOND: 48735.5 MH/S
W001 TIME SPENT/STEP: 10 MINUTES, 29 SECONDS (LENGTH=8)
W001 TIME LEFT: 1 HOUR, 38 MINUTES
W001 KEYSPEACE SEARCHED: 9.59%
W001 STATUS: RUNNING
W001 RECOVERED HASHES: 8659
W001 VALID HASHES LEFT: 38
W001 CUMULATIVE TIME: 25 MINUTES, 16 SECONDS
W001 === REALTIME DATA FOR CURRENT STEP END ===
    
```

Refresh

2021-01-31 07:04 CET *i*
© 2011-2020 Praetors AG 1.0.38

NTLM: Full Audit

Mixed Case

Standard Character Set

12-Character Password

Users: 10,000

Performance: ~80% in 2 hours

Worker: 1 x Nvidia 3090 GPU

NTLM: Results



NTLM: Full Audit

Mixed Case

Standard Character Set

12-Character Password

Users: 10,000

Performance: ~80% in 2 hours

Worker: 1 x Nvidia 3090 GPU

KDFAES: Use Results from NTLM as Wordlist

Editing Profile

https://epas-lab.detack.de/jobsettings.php?action=profileedit

epas

- Dashboard
- Targets
- Audit Jobs**
 - Jobs List
 - New Job
 - Audit Profiles
 - New Audit Profile
 - Settings
- Analysers
- Enforcer
- Reports
- System
- Logout

Preliminary Audit - RACF Passwords Normal Demo K
Required fields are marked with an asterisk(*)

Known Information

Time limit * 2:00 *i*

Initial passwords ☐ *i* Account information ☐ *i* Collected texts ☐ *i* **Collected passwords ☒ *i***

Rules enabled ☒ *i*

GPU rule set * G01_SMALL *i*

Hybrid enabled ☐ *i*

Fast Brute Force

Enabled ☐ *i*

Time limit * 2:00 *i*

Max length * 0 *i*

Select character sets

Name	Entries	Selected
Alpha (7-bit)	52	<input type="checkbox"/>

2021-01-31 20:26 CET *i*
© 2011-2020 Praetors AG 1.0.38

KDFAES: Preliminary Audit

Upper Case

Standard Character Set

8-Character Password

Users: 100

Dictionary: 8,661

Worker: 1 x Nvidia 3090 GPU

KDFAES: Results

epas Jobs - View Audit Log

https://epas-lab.detack.de/job.php?action=log&id=4

Dashboard

Targets

Audit Jobs

Jobs List

New Job

Audit Profiles

New Audit Profile

Settings

Analysar

Enforcer

Reports

System

Logout

2021-01-31 20:29 CET

© 2011-2020 Praetors AG 1.0.38

Main Job Log Return to List

Job Actions

Run Now Stop Running Job Interrupt Step Suspend Job Resume Job Clone Job Clear History Delete

Master Log

```

=== 01/31/2021 20:27:23 Queue processor is dispatching job 4 "RACF-KDFAES-ZOS21"
=== 01/31/2021 20:27:23 Allocated worker system with serial number "FBE1-B196-7AB8-35C9"
=== 01/31/2021 20:27:23 New audit job is being dispatched
=== 01/31/2021 20:27:26 Using EPAS password vault for target credentials
=== 01/31/2021 20:27:26 Extracting target data disabled, using last session
=== 01/31/2021 20:27:27 Password hashes retrieved: 100
=== 01/31/2021 20:27:27 Preparing preliminary mode
=== 01/31/2021 20:27:27 Site information words: 8661
=== 01/31/2021 20:27:27 Started all worker processes
    
```

Worker Log

```

W001 01/31/2021 20:28:25 PRELIMINARY MODE: STARTING KNOWN SITE INFORMATION STRAIGHT
DICTIONARY STEP
W001 01/31/2021 20:28:25 TIME LIMIT FOR THIS STEP 01:00:00
W001 01/31/2021 20:28:42 CURRENT STEP PASSWORDS/SECOND: 65215 H/S
W001 01/31/2021 20:28:42 CURRENT STEP TIME SPENT: 17 SECONDS
W001 01/31/2021 20:28:42 CURRENT STEP KEYSACE SEARCHED: 100.00%
W001 01/31/2021 20:28:42 CURRENT STEP ENDED WITH STATUS: COMPLETE
W001 01/31/2021 20:28:42 CUMULATIVE TIME SPENT: 1 MINUTE, 15 SECONDS
W001 01/31/2021 20:28:42 NO MORE HASHES LEFT. AUDIT STEP FINISHED
W001 01/31/2021 20:28:42 RESETTING HARDWARE COOLING
    
```

Refresh

KDFAES: Preliminary Audit

Upper Case

Standard Character Set

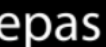
8-Character Password

Users: 100

Dictionary: 8,661

Performance: 100% in 2 min

Worker: 1 x Nvidia 3090 GPU



epas

- Dashboard
- Targets
- Audit Jobs
- Analyser
- Enforcer
- Reports
- Password Audit Reports
 - Aggregated Report Data
 - Password Reuse Reports
 - Reporting Options
- System
- Logout

Password Audit Report

ZOS21 : 10.222.224.180
Executive Summary

1. Audit Summary

This report comprises the results of the password security audit which was performed against the target system presented below. This section contains the top level information concerning the audit and the results, as well as the licensing information, if applicable.

Data retrieval date	2021-01-31 2:26
Password audit start	2021-01-31 20:27
Password audit end	2021-01-31 20:29
Job duration (H:M:S)	0:02:05
Total accounts on target	289
Passwords audited	100
Passwords recovered	100 (100%)
Audit job name	RACF-KDFAES-ZOS21 [Link]
Reporting group	Unrestricted [Change]

2. Target and Audit Profile Information

This section contains the target system data and the audit job profile parameters.

Target system name	ZOS21 [Link]
Target system type	IBM System z - zSeries - z/OS RACF
IP Address	10.222.224.180
Password policy name	No policy selected for this audit.
Audit profile name	RACF Passwords Normal Demo K [Link]
Collect texts enabled	No
Collect passwords enabled	No
Anonymize accounts	No
Accounts filter enabled	Yes

2021-01-31 20:30 CET ⓘ
© 2011-2020 Praetors AG 1.0.38

Worker: 1 x Nvidia 3090 GPU

In Brief

- Attacks against password hashes on RACF are still possible, but harder and yield less cracked passwords
- As long as weaker systems exist in the environment, “a chain is only as strong as its weakest link”
- Mainframe security efforts no longer make sense isolated from the rest
- Password cracking is usually NOT the way mainframes are hacked, but it is in 90% of the cases instrumental, so make sure strong passwords are used, and are not the same or similar to other, weaker systems
- Password spraying can be used to hack mainframes too, so make sure that leaked passwords are detected
- N.B. RRSF: Make sure all systems use KDFAES, as the password is transmitted in clear text and hashed by each RACF instance separately with KDFAES or DES, as configured.

Questions we ask ourselves ...

1. Have you encountered any real life cases where password cracking of exposed RACF db was the reason, or at least instrumental in a successful mainframe security attack (no names)? How about employing such methods yourself as an auditor / penetration tester?
2. Password spraying, and leaked passwords in general: what is the actual danger, and what is the awareness we have today in enterprises, in general, but also specifically for mainframe users? Would alerting prevent such an attack?
3. Stronger password hashing: Are we better off now? Hash cracking is only a matter of interest if the RACF database is exposed. Does it help security, by making the system safer, does it help people to use weaker passwords undetected by analytics tools?
4. Adding another factor besides the password would make things more secure, at least for interactive users. Is IBM MFA AZF????1 getting any traction? Acceptance is bad amongst users, PSD2 has been challenged in Germany, do we know of any adaptive/conditional authentication for RACF?
5. Obscurity vs. security, would it make sense that intended changes in password crypto is based on standards and fully disclosed, instead of keeping it secret? Would eliminating potential mistakes – see the DES password phrases – outweigh the potential / imaginary risks or disclosing the algo?