Forage

THE BEST RUN SAP®

SAP CYBERSECURITY VIRTUAL INTERNSHIP PROGRAM

Task 1 - Protect the keys to the kingdom!

Identify password flaws for your client's most sensitive accounts.

Pablo Gagliardi

THE BEST RUN SAP®

Forage

NIST Special Publication 800-53B Appendix A review.

Mon, 21 Jun 2021 08:23:00 -0400

NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

Appendix A—Strength of Memorized Secrets

The text provides informative details about the strength of passwords and how they can be improved to enhance security. The author starts by discussing the limitations of humans in memorizing complex and arbitrary passwords, and how online services have introduced rules to increase the complexity of passwords. However, the author notes that composition rules such as requiring a mix of character types may not be effective as users tend to choose predictable passwords.

The author then discusses the importance of password length in determining password strength. Passwords that are too short are vulnerable to brute force and dictionary attacks, and a minimum password length should be required depending on the threat model being addressed. The author also notes that offline attacks are sometimes possible when hashed passwords are obtained by attackers through a database breach.

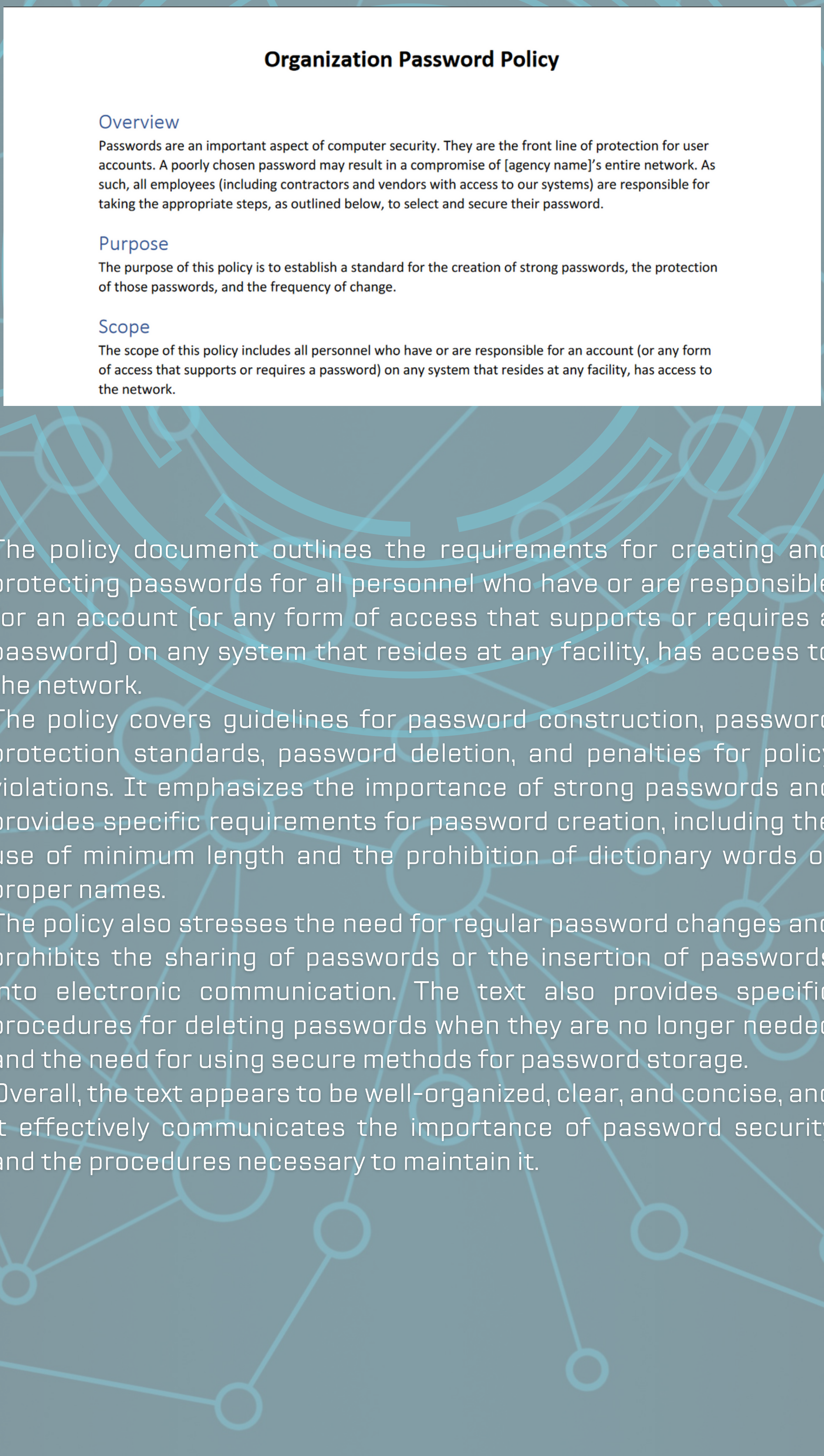
The author recommends that users should be encouraged to make their passwords as lengthy as they want, within reason. However, extremely long passwords may require excessive processing time to hash. The author also suggests that passwords chosen by users should be compared against a "blacklist" of unacceptable passwords, including those from previous breaches and dictionary words.

The author concludes by noting that highly complex passwords may be less memorable and more likely to be written down or stored electronically in an unsafe manner. Overall, the text provides valuable information and recommendations to improve password strength and enhance security.

THE BEST RUN SAP®

Forage

Organization Password Policy review.



The policy document outlines the requirements for creating and protecting passwords for all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any facility, has access to the network.

The policy covers guidelines for password construction, password protection standards, password deletion, and penalties for policy violations. It emphasizes the importance of strong passwords and provides specific requirements for password creation, including the use of minimum length and the prohibition of dictionary words or proper names.

The policy also stresses the need for regular password changes and prohibits the sharing of passwords or the insertion of passwords into electronic communication. The text also provides specific procedures for deleting passwords when they are no longer needed and the need for using secure methods for password storage.

Overall, the text appears to be well-organized, clear, and concise, and it effectively communicates the importance of password security and the procedures necessary to maintain it.

THE BEST RUN SAP®

Forage

compliant and non-compliant users

GivenName	MiddleInitial	Surname	StreetAddress	City	State	ZipCode	EmailAddress	Username	Password	TelephoneNumber
Charles	D	Alexander	2088 Hillside Drive	Cambridge	MA	12141	CharlesDAlexander@clientdomain.com	Othy1935	XDMSjLvWgGF	339-814-9960
John	J	Jones	1501 Copperhead Road	Farmington	CT	16032	JohnJJones@clientdomain.com	Hustry	bmVcKzWphuS	860-678-5692
Erika	N	Ransdell	174 Caldwell Road	Fairport	NY	14450	ErikaNRansdell@clientdomain.com	Chustered1993	$FwM3Hs+taev2*%f	585-267-6077
Frank	E	Helmick	3216 Harley Brook Lane	Erie	PA	16501	FrankEHelmick@clientdomain.com	Auneance	q$_pL/6!D%?9(vXn	814-528-2078
Christopher	C	Hale	2900 Golf Course Drive	Washington	VA	20011	ChristopherCHale@clientdomain.com	Fintich	+6W=F&LTK@c>2t?Z	703-342-1511
Mary	D	Silva	325 Green Gate Lane	Chantilly	MD	20151	MaryDSilva@clientdomain.com	Laine1948	btwWeJxshSn	443-726-6761
Billie	R	White	4501 Cabell Avenue	Beltsville	VA	20705	BillieRWhite@clientdomain.com	Hincycle	xwvr6X+KyY}c(Nmf	703-599-0791
Patricia	F	Cochran	201 Jennifer Lane	Raleigh	NC	27616	PatriciaFCochran@clientdomain.com	Seench	9(Cy8S=@)aPws[Lc	919-439-5005
Linda	S	Castle	2363 Stratford Court	Durham	NC	27701	LindaSCastle@clientdomain.com	Paptur	+E7R2f*=HvrS>gqX	919-688-0995
Gloria	W	Hicks	1108 Arbutus Drive	Miami Springs	FL	33166	GloriaWHicks@clientdomain.com	Thfuld51	ejXPHvyabUC	305-840-2808
Julia	A	Matthews	3985 Warner Street	North Dade	FL	33180	JuliaAMatthews@clientdomain.com	Ature1979	=gHEY+-&9w!(_^P7	305-935-6701
Heather	T	Marquez	81 Duffy Street	Hammond	IN	46323	HeatherTMarquez@clientdomain.com	Coused36	9MBt{GeN}L>5j]mC	219-838-2166
Florence	M	Landers	2207 Tuna Street	Southfield	MI	48075	FlorenceMLanders@clientdomain.com	Nessichaved	WuPxGRFEbTn	810-937-3404
Angela	J	Patton	1264 Ashwood Drive	Council Bluffs	IA	51501	AngelaJPatton@clientdomain.com	Patern	!z>.K/5sR}7Nb(]V	712-366-4638
Carl	E	Young	4821 Bailey Drive	Iowa City	IA	52240	CarlEYoung@clientdomain.com	Tentme1953	uZPX=VSs$E_2-{]^	319-356-1580
Keith	G	Zamora	2519 Reeves Street	Lena	WI	54139	KeithGZamora@clientdomain.com	Nect1952	Z-p]xSTGNqz%Ck(2	920-829-1007
Ted	L	White	706 Pineview Drive	Marshall	MN	56258	TedLWhite@clientdomain.com	Meman1989	UBTNjzkWQbr	507-929-2767
Dustin	L	Sigler	2947 North Avenue	Giltner	NE	68841	DustinLSigler@clientdomain.com	Priefichat	R9p>ncEbNy4A@GL3	402-849-0966
Catherine	O	Merritt	3906 Emerson Road	Dubach	LA	71235	CatherineOMerritt@clientdomain.com	Sartury	LDsHcfxtbph	318-777-9992
Inez	H	Waters	1517 Whispering Pines Circle	Dallas	TX	75240	InezHWaters@clientdomain.com	Heach1976	TszYCSULvBd	972-362-8121
Martin	E	McBride	4409 Parrish Avenue	San Antonio	TX	78205	MartinEMcBride@clientdomain.com	Namen1973	L7dxqz%.u(8NDX+J	830-848-2671
Betty	W	House	2915 Logan Lane	Denver	CO	80221	BettyWHouse@clientdomain.com	Plabou	Hwr6SQjbsE.k>@42	303-262-0686
Duane	H	Rapoza	4615 Clarksburg Park Road	Yuma	AZ	85365	DuaneHRapoza@clientdomain.com	Motersight	4VmANX3W5+Z=FqT8	928-317-5460
Gerald	J	Mosqueda	3464 Euclid Avenue	Los Angeles	CA	90014	GeraldJMosqueda@clientdomain.com	Asaing	mfLGjazFtuk	805-299-8864
Roy	C	Kellogg	3535 Poplar Avenue	San Diego	CA	92111	RoyCKellogg@clientdomain.com	Clat1979	rgvBW]t7}V5+)D=N	619-540-6270
Cathy	R	Frisbie	880 Kerry Way	Irvine	CA	92614	CathyRFrisbie@clientdomain.com	Hime1979	bHwdmXnYMPF	562-832-0226
Denise	J	Gaston	877 Norman Street	Irvine	CA	92614	DeniseJGaston@clientdomain.com	Ingdp1999	RE6QPsZY8Au9!5h_	323-304-5111
John	K	Lemon	1924 Angie Drive	Santa Ana	CA	92701	JohnKLemon@clientdomain.com	Doreas73	=t_nX7[(B)zq]CaW	714-972-1259
Melissa	R	Lubin	848 Jim Rosa Lane	San Francisco	CA	94107	MelissaRLubin@clientdomain.com	Compt1936	hUVJcMLSR7D]tz-4	415-816-0851
Mimi	E	Faulkner	4389 Timbercrest Road	Circle	AK	99733	MimiEFaulkner@clientdomain.com	Seepas	4HT&[^9rk}WVAq.Y	907-773-9186

According to the customer's password policy document, there are many users with passwords that do not meet the criteria. Many of the passwords are less than 12 characters, so it doesn't meet the minimum length criteria. None of the users use their user ID as a password or include words from the dictionary.

Users whose lines are pink do not comply, all have eleven-character passwords. The green lines are the compliant users.

Username	Password
Othy1935	XDMSjLvWgGF
Hustry	bmVcKzWphuS
Chustered1993	$FwM3Hs+taev2*%f
Auneance	q$_pL/6!D%?9(vXn
Fintich	+6W=F&LTK@c>2t?Z
Laine1948	btwWeJxshSn
Hincycle	xwvr6X+KyY}c(Nmf
Seench	9(Cy8S=@)aPws[Lc
Paptur	+E7R2f*=HvrS>gqX
Thfuld51	ejXPHvyabUC
Ature1979	=gHEY+-&9w!(_^P7
Coused36	9MBt{GeN}L>5j]mC
Nessichaved	WuPxGRFEbTn
Patern	!z>.K/5sR}7Nb(]V
Tentme1953	uZPX=VSs$E_2-{]^
Nect1952	Z-p]xSTGNqz%Ck(2
Meman1989	UBTNjzkWQbr
Priefichat	R9p>ncEbNy4A@GL3
Sartury	LDsHcfxtbph
Heach1976	TszYCSULvBd
Namen1973	L7dxqz%.u(8NDX+J
Plabou	Hwr6SQjbsE.k>@42
Motersight	4VmANX3W5+Z=FqT8
Asaing	mfLGjazFtuk
Clat1979	rgvBW]t7}V5+)D=N
Hime1979	bHwdmXnYMPF
Ingdp1999	RE6QPsZY8Au9!5h_
Doreas73	=t_nX7[(B)zq]CaW
Compt1936	hUVJcMLSR7D]tz-4
Seepas	4HT&[^9rk}WVAq.Y

THE BEST RUN SAP®

Forage

compliant and non-compliant users

Something extra:

We can check if the passwords match the criteria using a bash script:

```
#!/bin/bash

# Define the regular expressions for password validation
regex_length=".{12,}"
regex_username="^(?i)(.*)\\1$"
regex_dict="^((?i)admin|password|123456|qwerty|letmein)$"
regex_name="^((?i)james|john|robert|michael|william)$"

# Read the input file and process each line
while read line; do
  # Split the line into fields using commas as the delimiter
  IFS=',' read -ra fields <<< "$line"

  # Get the username and password fields
  username="${fields[9]}"
  password="${fields[10]}"

  # Check the length of the password
  if [[ ! $password =~ $regex_length ]]; then
    echo "Password for user ${fields[8]} is too short"
    fields+=("too short") # Add "too short" to the end of the array
  # Check if the password is the same as the username
  elif [[ $password =~ $regex_username ]]; then
    echo "Password for user ${fields[8]} cannot be the same as username"
    fields+=("same as username") # Add "same as username" to the end of the arra
  # Check if the password is a dictionary word or proper name
  elif [[ $password =~ $regex_dict || $password =~ $regex_name ]]; then
    echo "Password for user ${fields[8]} is not secure"
    fields+=("not secure") # Add "not secure" to the end of the array
  else
    echo "Password for user ${fields[8]} is valid"
    fields+=("valid") # Add "valid" to the end of the array
  fi

  # Join the fields back into a comma-separated string
  new_line=$(IFS=','; echo "${fields[*]}")

  # Append the new line to the output file
  echo "$new_line" >> output.csv

done < ClientADIdentities.csv
```

THE BEST RUN SAP®

Forage

Compliant and non-compliant users

Something extra:

Explanation of the script:

- Three regular expressions are defined to check the length of the password, whether the password is the same as the username, and whether the password is a dictionary word or proper name.
- The while loop reads each line from the input file (ClientADIdentities.csv) and processes it.
- The read command splits each line into fields using commas as the delimiter and stores them in an array (fields).
- The username and password fields are extracted from the array (username="${fields[9]}" and password="${fields[10]}"), assuming that the username and password fields are the 10th and 11th fields in the input file.
- The length of the password is checked against the regular expression for password length (regex_length) using the !~ operator. If it does not match, a message is printed indicating that the password is too short, and the string "too short" is added to the end of the array (fields+=("too short")).
- The password is checked against the regular expression for username (regex_username) using the =~ operator. If it matches, a message is printed indicating that the password cannot be the same as the username, and the string "same as username" is added to the end of the array (fields+= ("same as username")).
- The password is checked against the regular expressions for dictionary words and proper names (regex_dict and `regex