How Forced Password Expiration Affects Password Choice

By Bruce K. Marshall - @PwdRsch

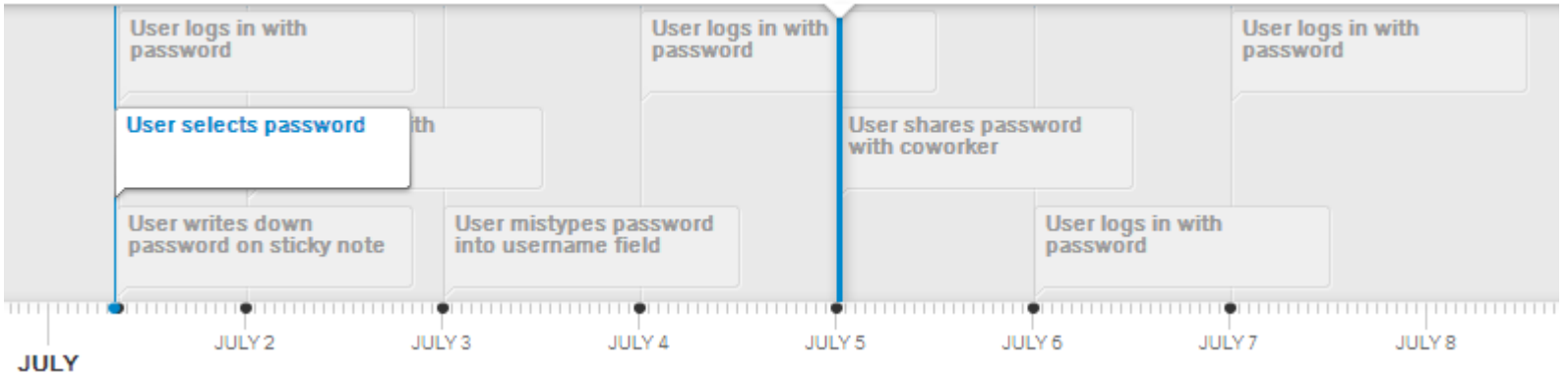
Passwords Are Most Effective When Kept Secret

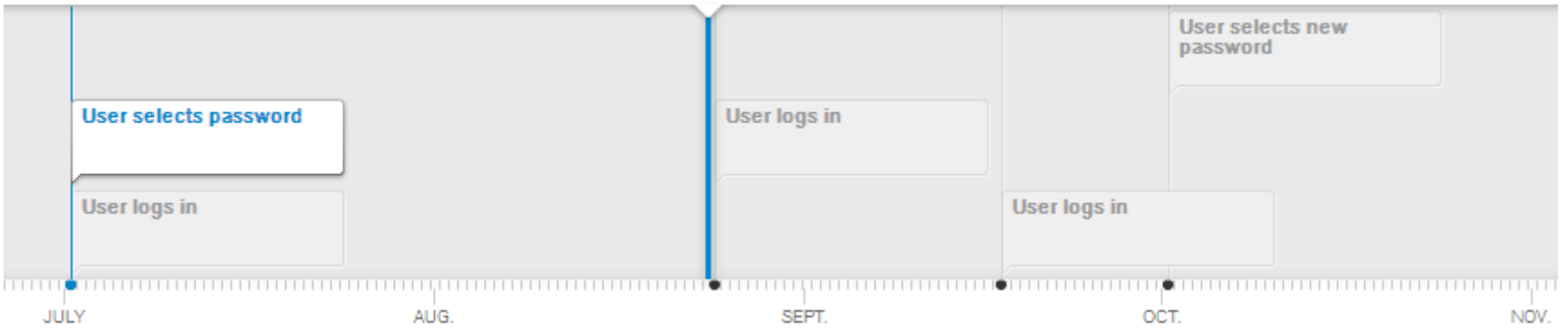
If a password is compromised by an unauthorized individual, change it.

If a password is suspected to be compromised by an unauthorized individual, change it.

If a password has been used long enough or in risky enough situations that compromise is possible, change it.

Password Use Timeline





Do People Change Passwords When Informed of Compromise?

If you read/hear that a business that you have a personal account with has been hacked, how long do you wait before you change your password with that company?

- 80.1% - Immediately
- 4.1% - When I next use the account
- 3.5% - When I remember
- 3.6% - When I get a chance
- 0.8% - I don't change my password
- 7.8% - It hasn't happened to me

Source: Siber Systems RoboForm Online Security Survey (2012)

Do People Change Passwords When Informed of Compromise?

Univ. of Delaware sent out notice to students and staff that they should change their primary network passwords due to the Heartbleed vulnerability

- 2 weeks later 8,300 students and 3,600 employees had changed passwords on their own
- Approximately 16,000 (57%) more students/staff had not changed their password since the announcement and were going to be subjected to forced changes

Source: http://www.udel.edu/udaily/2014/apr/passwords-042514.html

Do People Change Passwords When Informed of Compromise?

Ebay experienced security breach on May 21 that they say compromised their 'encrypted' password database. Customers were advised to change passwords via email

- 9 weeks later Ebay CEO said that “buyers representing roughly 85% of "effective volumes" on its platform” had changed passwords on their own

Source: http://mobile.reuters.com/article/idUSL2N0PR2Q220140716?irpc=932

What Do We Know About Password Compromise Timelines?

Example 1 - The Onion

- May 3, 2013 – SEA sends phishing emails to Onion staff that prompted for Google credentials
- May 6, 2013 – After one successful phish they use that employees account to send out further phishing emails
- May 6? 2013 – Two more successfully phished, one of whom had social media account access
- May 6? 2013 – Faked password reset email sent from employee provided continued access

What Do We Know About Password Compromise Timelines?

Example 2 - South Carolina Dept of Revenue

- Day 1 – Phishing email with credential capturing trojan sent to multiple employees
- Day 15 – Attackers use captured credentials to access internal network and find other systems
- Day 17 – Attackers steal 6 more passwords
- Day 20 – Attackers steal passwords for “all windows accounts” & install backdoor

What Do We Know About Password Compromise Timelines?

Example 3 – Israel Institute of Technology

- Hacker showed off to journalist that he could log into the account of the Computer Advisory Centre director
- Director confirmed that compromised password hadn't been changed in the 4 years since the hacker had originally obtained it (unbeknownst to the director)

Enter Password Expiration/Aging

- Goal #1 - A password should be replaced before it is likely to be compromised
- Goal #2 - Remove value associated with knowledge of the old password
- Typically a policy-driven control that is triggered after the password has been used for an established period of time
- May require password change ahead of expiration date or might allow 'grace' login

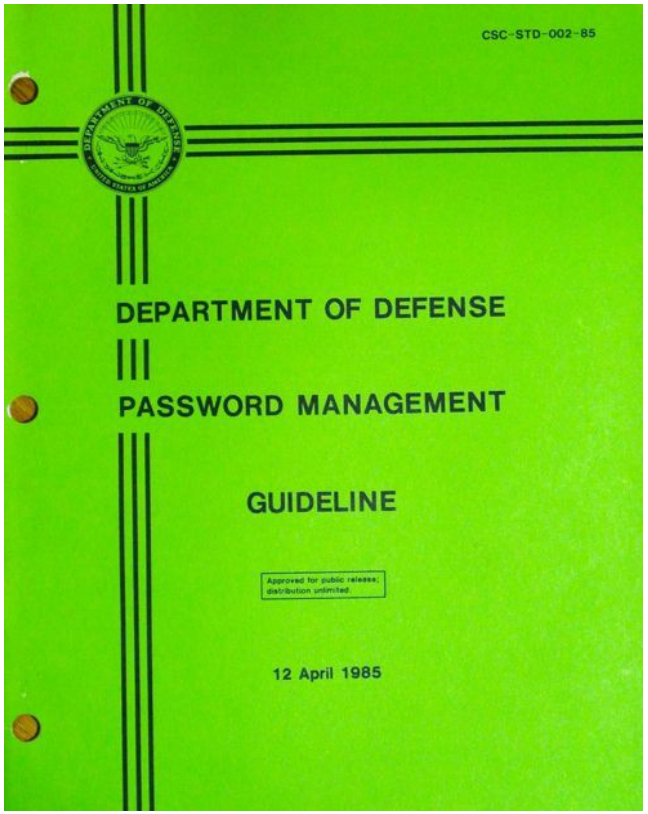
Controls That Accompany Expiration

- Password History – Record of X previous passwords used by the account
- Minimum Password Age – How much time must elapse after a password change before that user can initiate another change on their own
- Change Notification – System alert, email, or message that lets a user know that their password is going to expire soon

Where Do Password Expiration Guidelines Come From?

- “[Passwords] should be changed often enough so that there is an acceptably low probability of compromise during a password's lifetime.”

- “There should be a maximum lifetime for all passwords. To protect against unknown threats, it is recommended that the maximum lifetime of a password be no greater than 1 year. The presence of known threats may indicate a need for a shorter maximum lifetime.”



Sources of Support for Password Expiration

- Microsoft
  - Windows 2000 domain policy, when enabled, defaulted to 42 days; Account Lockout Best Practices White Paper (2003)
  - Windows 2000 Evaluated Configuration Administrators Guide (2002) - “Where security is a concern, good values are 30, 60, or 90 days. Where security is less important, good values are 120, 150, or 180 days."
  - Microsoft Windows 2000 Security Hardening Guide (2003) - 70 days

Sources of Support for Password Expiration

- PCI Council Data Security Standard (2004/2013)
  - Section 8.2.4 - “Change user passwords/ passphrases at least every 90 days.” Applies to non-consumer users.

- SANS Critical Security Controls (2009)
  - Control 16-8 says “Require that all non-admin accounts have strong passwords that ... be changed at least every 90 days, have a minimal age of one day ... These values can be adjusted based on the specific business needs of the organization.”

Sources of Support for Password Expiration

- HIPAA
  - Security Rule just says in title 45 CFR part 164.308(a)(5)(ii)(D) to establish "Procedures for creating, changing, and safeguarding passwords."
  - HIPAA Security Information Series Part 2 doc (2005/2007) from the HHS - "Covered entities must train all users and establish guidelines for creating passwords and changing them during periodic change cycles."

Sources of Support for Password Expiration

- OWASP
  - Application Security Verification Standard (2013) requirement V1.13 - "Verify authentication credentials can expire after an administratively configurable periods of time."
  - Web site: “The recommendation that users change their passwords regularly and do not reuse passwords is universal among security experts.”

Sources of Support for Password Expiration

- FFIEC
  - IT Examiners Handbook (undated) - "Shared secret strength is typically assured through the use of automated tools that enforce the password selection policy. Authentication systems should force changes to shared secrets on a schedule commensurate with risk."

Sources of Support for Password Expiration

- NIST
  - 800-118 - Guide to Enterprise Password Management (2009) - “Organizations should decide whether to use password expiration mechanisms and what expiration period to set based on balancing security needs and usability. [C]onsider having different policies for password expiration for different types of systems, OSs, and applications, to reflect their varying security needs and usability requirements.”

Sources of Support for Password Expiration

- ISO/IEC
  - 17799-2005 Code of Practice for Information Security Management Section 11.3.1 - "All users should be advised to: change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid reusing or cycling old passwords"
  - Section 11.5.3 - "A password management system should: enforce password changes;"

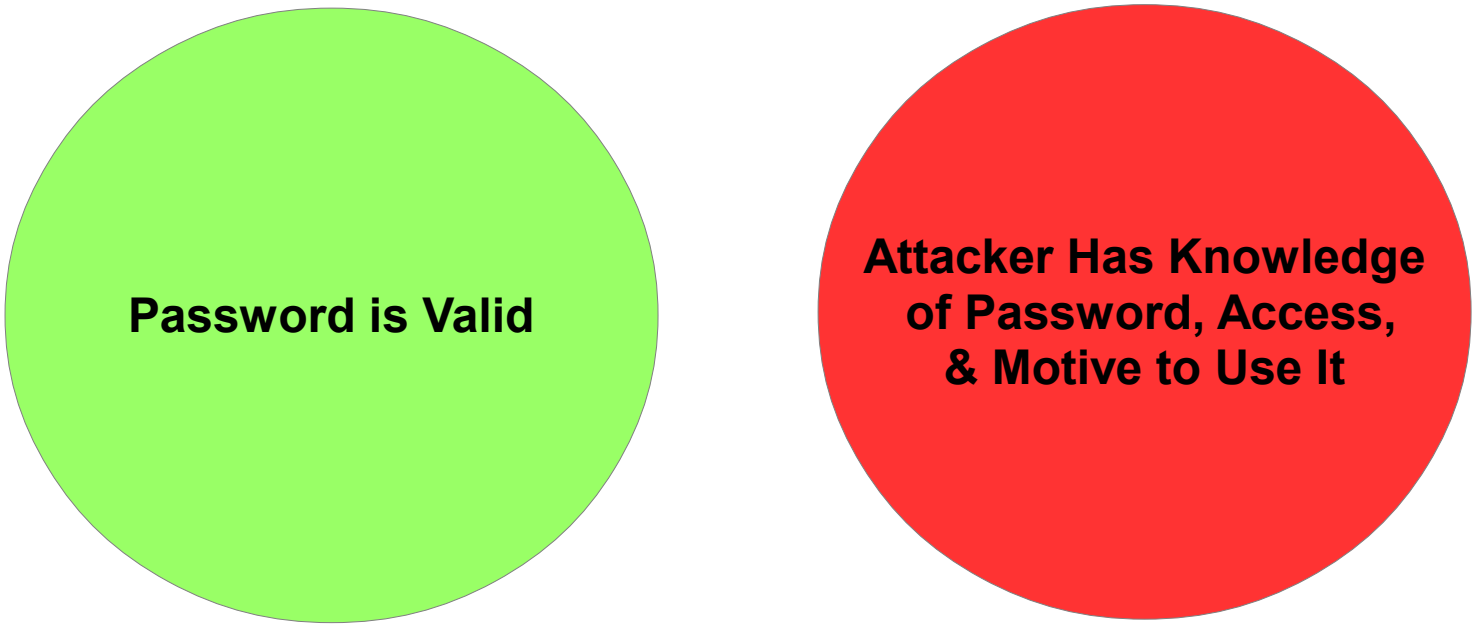
Sources of Support for Password Expiration

- ISO/IEC (continued)
  - 27002-2013 Code of Practice for Information Security Management Section 9.3.1 (maps to previous 11.3.1) removes instruction for users to regularly change passwords
  - Section 9.4.3 (maps to previous 11.5.3) says: "A password management system should: enforce regular password changes as needed;”

Sources of Support for Password Expiration

- Analysis of End User Security Behaviors (2004)
  - Surveyed 49 information technology students with MS or PhD on a variety of user security behaviors. They were provided with a statement and asked to rate it on both intentions (malicious or benevolent) and expertise (novice and expert).
  - 39 out of 49 (80%) rated the statement “She did not change her password for over two years.” as “Naive Mistakes”.

How Password Expiration Affects Compromised Credential Use



How often does a password changed due to scheduled expiration thwart an attacker using it or continuing to use it?

What Does The Average Person Think About Changing Passwords?

- “38% would rather undertake household chores, like cleaning the toilet or doing the dishes, than have to create another username and password” – Jainrain Online Registration and Password (2012)
- People were asked how they felt about the statement “Do not trust systems or websites that do not require frequent password changes.” Around 38% and 37% of US and UK residents, respectively, said they agreed or strongly agreed. – Ponemon Institute report Moving Beyond Passwords: Consumer Attitudes on Online Authentication (2013)

User Approaches to Dealing with Password Expiration

Viki Tucker
@MothaTuckaaa

I hate how often I have to change my password for school.. I'm running out of passwords

11:54 AM - 20 Aug 2013

Jazmine Chance
@hugableprincezz

@MothaTuckaaa change the number +1 like password1 to password2.....works everytime

1:04 PM - 20 Aug 2013

Scott
@scottsues

@samwdowning i was embarrassed with my old password policy which was "ilovesam1" and i just updated the number every month.

8:53 PM - 3 Jun 2014

Alisha Laferty
@leasherr

Just remembered that my osu password expired today... Time to think of a new one #gettinghard

9:10 PM - 25 Jun 2014

mark
@carkmaldwell

@leasherr just change it to the date like June252014

9:15 PM - 25 Jun 2014

Sydney Aten
@sydaten13

OSU's tri-monthly password reset---aka how long will it take until I run out of symbols to string onto the end of the same word

7:29 PM - 2 Jul 2014

Sources of Criticism for Password Expiration

"Most UNIX systems are provided with a feature called password aging, which, if activated by the system administrator, will cause users of the system to change their passwords every so often. The goal is laudable. The algorithm, however, is bad, and the implementation, from a security standpoint, is just awful."

– Fred T. Grampp & Robert H. Morris, The UNIX System: UNIX Operating System Security (1984)

Sources of Criticism for Password Expiration

"For many years I have been seeking a scientific basis for the well-worn policy of changing passwords on a regular basis. Recently, I have come to believe that, except in some special cases, this is not a beneficial activity for information security and that it is devoid of a scientific basis."

– Fred Cohen, Change Your Password - Doe See Doe (1997)

Sources of Criticism for Password Expiration

- Richard E. Smith - Authentication: From Passwords to Private Keys book (2001)
- Mark Burnett - Perfect Passwords book (2005)
- Ray Wagner, Ant Allan, & Jay Heiser (Gartner) - Eight Security Practices Offer More Value than Password Aging (2005)
- Steve Bellovin (Univ. of Columbia) - Unconventional Wisdom (2006)
- Gene Spafford (Purdue Univ) - Security Myths & Passwords (2006)

Sources of Criticism for Password Expiration

- Ari Juels (RSA) – Password Expiration: Like Margarine and Water (2008)
- Ross J. Anderson (Univ. of Cambridge) - Security Engineering: A Guide to Building Dependable Distributed Systems 2E (2008)
- Bruce Schneier (BT Counterpane) - Changing Passwords (2010)
- Dan Auerbach & Seth Schoen (EFF) - Passwords: LinkedIn And Beyond (2012)

UNC Study of Password Expiration

- The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis (2010), by Zhang, Monrose, Reiter
- Analyzed password histories of 7,700 disabled accounts at Univ. North Carolina – Chapel Hill
- Passwords expired every three months
- Passwords complexity: must contain at least 1 letter, 1 digit, and 1 special character (16 available, mostly shift-#)

UNC Study of Password Expiration

- Used transform based guessing against an old passwords to see if it accurately matched a new password. Example:
  - s/1/2 Password1 > Password2
- Found that 41% of new passwords could be broken offline from old using < 550 transforms
- Average of 17% new passwords could be broken using only the top 5 popular transforms

Zulu Case Study

- Corporate Active Directory environment where three samples of password hashes were taken over a 3 year period
  - Year 1 = 4,511 accounts/passwords
  - Year 2 = 5,021 accounts/passwords
  - Year 3 = 2,064 accounts/passwords
- No password expiration or complexity required
- Minimum length: 3

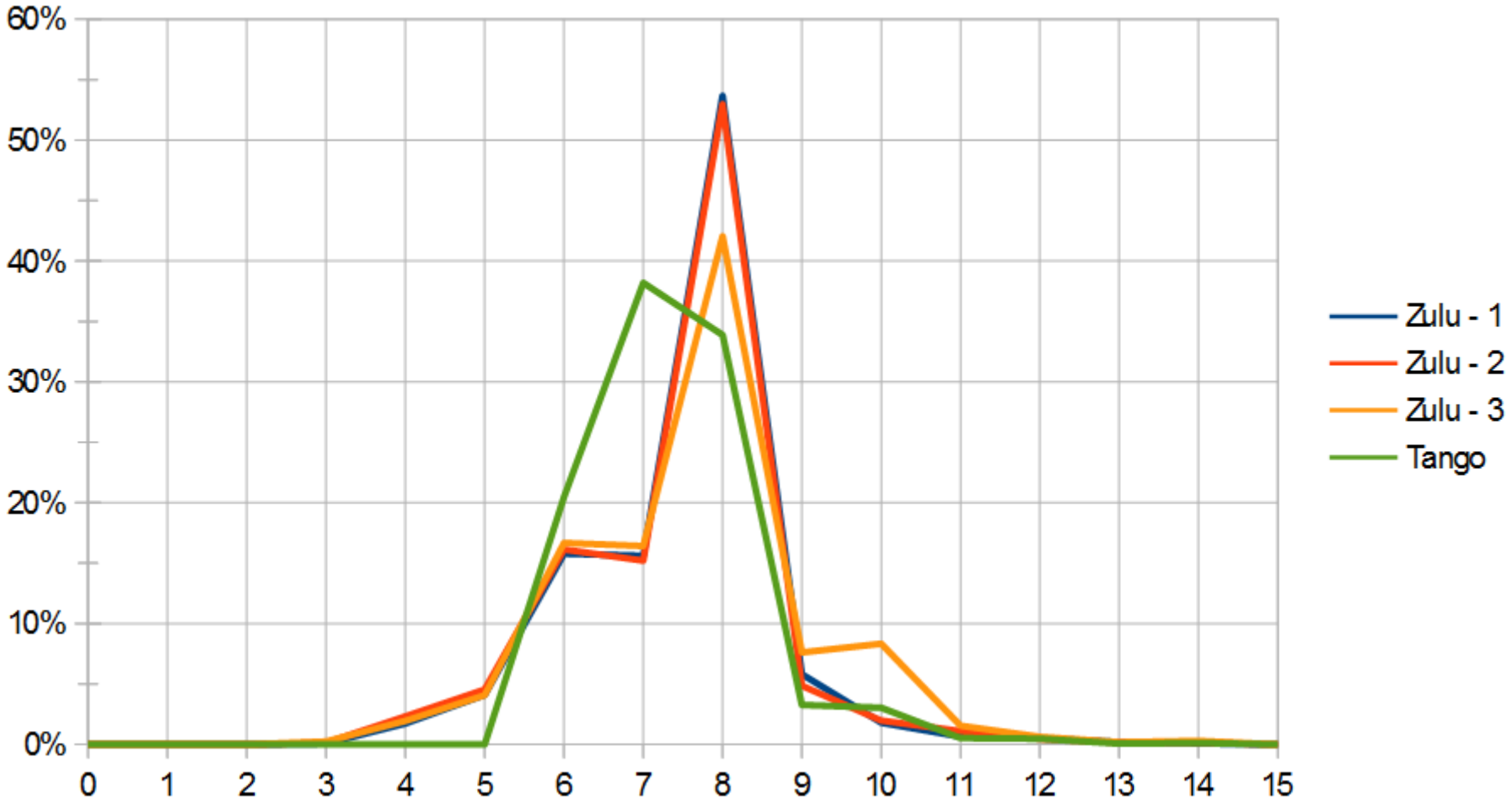
Zulu Case Study
Password Changes

- What percent of passwords changed over 3 years?
  - Year 1 – 2 = Duplicate accounts with the same password: 83%
  - Year 2 – 3 = Duplicate accounts with the same password: 81%
  - Accounts with at least 2 different passwords: 25%
  - Accounts with at least 3 different passwords: 4%
- Why would these people change passwords?

Tango Case Study

- Corporate Active Directory environment where single sample in time was taken. Consisted of 1,715 cracked account passwords.
- Forced password changes every 30 days
- No password complexity required
- Minimum length: 6 characters

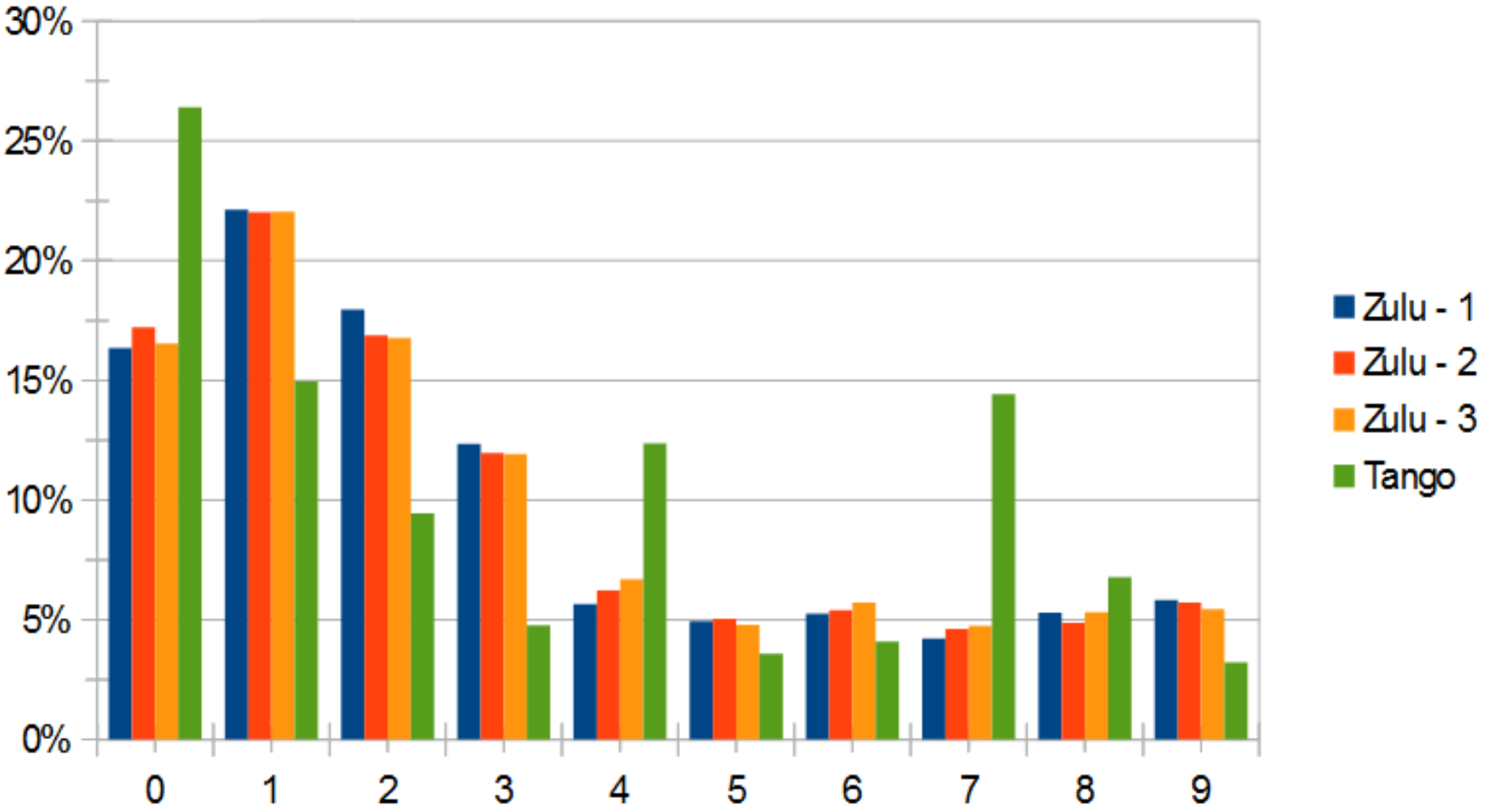
Password Length Comparison



Password Character Mask Comparison

Zulu - 3	Uniq Masks: 340	2,064	**Tango**	Uniq Masks: 137	1,715
Mask	Count	Percent	Mask	Count	Percent
lllllll	589	28.5%	llllln	396	23.1%
llllll	129	6.3%	lllllnn	395	23.0%
lllllll	123	6.0%	llllnn	133	7.8%
lllllllll	121	5.9%	lllllnn	107	6.2%
lllnnn	75	3.6%	lllll n	87	5.1%
llllllnn	58	2.8%	lllnnnn	68	4.0%
llllll n	52	2.5%	llllnnnn	64	3.7%
lllll	51	2.5%	lllllll n	37	2.2%
lllllll n	49	2.4%	llllll	34	2.0%
lllnnnn	47	2.3%	lllnnn	27	1.6%

Number Use Comparison



So Why Do Companies Insist on Password Expiration?

"Failing an audit is another kind of risk an enterprise has to mitigate. Hence, enterprises may choose to institute password management rules to satisfy auditors, even when they have no intrinsic value or, worse, when they can actually be deleterious (but failing the audit is seen as the bigger risk)."

– Ant Allan, Gartner – Best Practices for Managing Passwords: Policies Must Balance Risk, Compliance and Usability Needs (2010)

So Why Do Companies Insist on Password Expiration?

"How much mental anguish is the result of ignorant accounting grads working for Big 4s, struggling to find SOX-relevancy, totally oblivious to the huge amount of HCI research that has been done on the topics of passwords, so ignorant to the history of computer security that they don't recognize they are demanding the use of pre-network, pre-malware controls that were developed by mathematicians who were completely ignoring human factors."

– Jay Heiser, Research VP @ Gartner - Time For a Rant About Passwords (2011)

We're Also To Blame

- Being overly risk averse leads to controls like this becoming 'best practices'
- It's easy to ignore the need to reevaluate practices on a regular basis to see if they still make sense
- However, in less mature organizations password expiration is an easily enabled control that can fill in some gaps

News of Changes to Password Expiration Policies

- Emerson College eliminated password expiration for student accounts last year, only emailing encouragement to change them annually
- Cardiff University moving from 90 day to no expiration
- Northern Illinois University went from 130 to 265 days, but increased minimum length
- US Defense Finance & Accounting Service announced passwords will start expiring every 150 days instead of every 60

thelantern.com/2014/01/bob-gribben-takes-hatred-stride/

Bob Gribben takes 'hatred' in stride

January 16, 2014
Kristen Mitchell
mitchell.935@osu.edu

Students probably wouldn't recognize Bob Gribben around campus — but many know his name.

What they think of him, though, he described as "hatred."

A director of service operations in the Office of the Chief Information Officer, Gribben's name is tied to the emails reminding students and faculty to change their passwords every 90 days.

While the 90 day turnover is considered an industry best practice, Gribben said, that doesn't stop him from getting negative feedback.

"Faculty members are the ones that really email me and tell me, 'Hey listen, your policy is a disaster, how could you make us reset our password, all you're doing is creating an environment that causes us to be insecure,'" Gribben said. "They would really write up this nice, long dissertation, and I don't have any control over it."

The 90-day policy was put in place about three years ago, and Gribben's name was put on the reminder emails to give it a

Bob Gribben, a director of service operations in the OCIO, poses for a photo Jan. 2. Gribben's name is tied to the emails reminding students and faculty to change their passwords every 90 days.
Credit: Kristen Mitchell / Editor-in-chief

Alternatives to Scheduled Password Expiration

- Force changes only when compromise is suspected, or password policy changes
- Intrusion prevention + behavioral profiling of user activity
- Better feedback to users on suspicious activity
- Not using passwords (or at least not using them as the primary authenticator)

Areas Where Research Is Needed

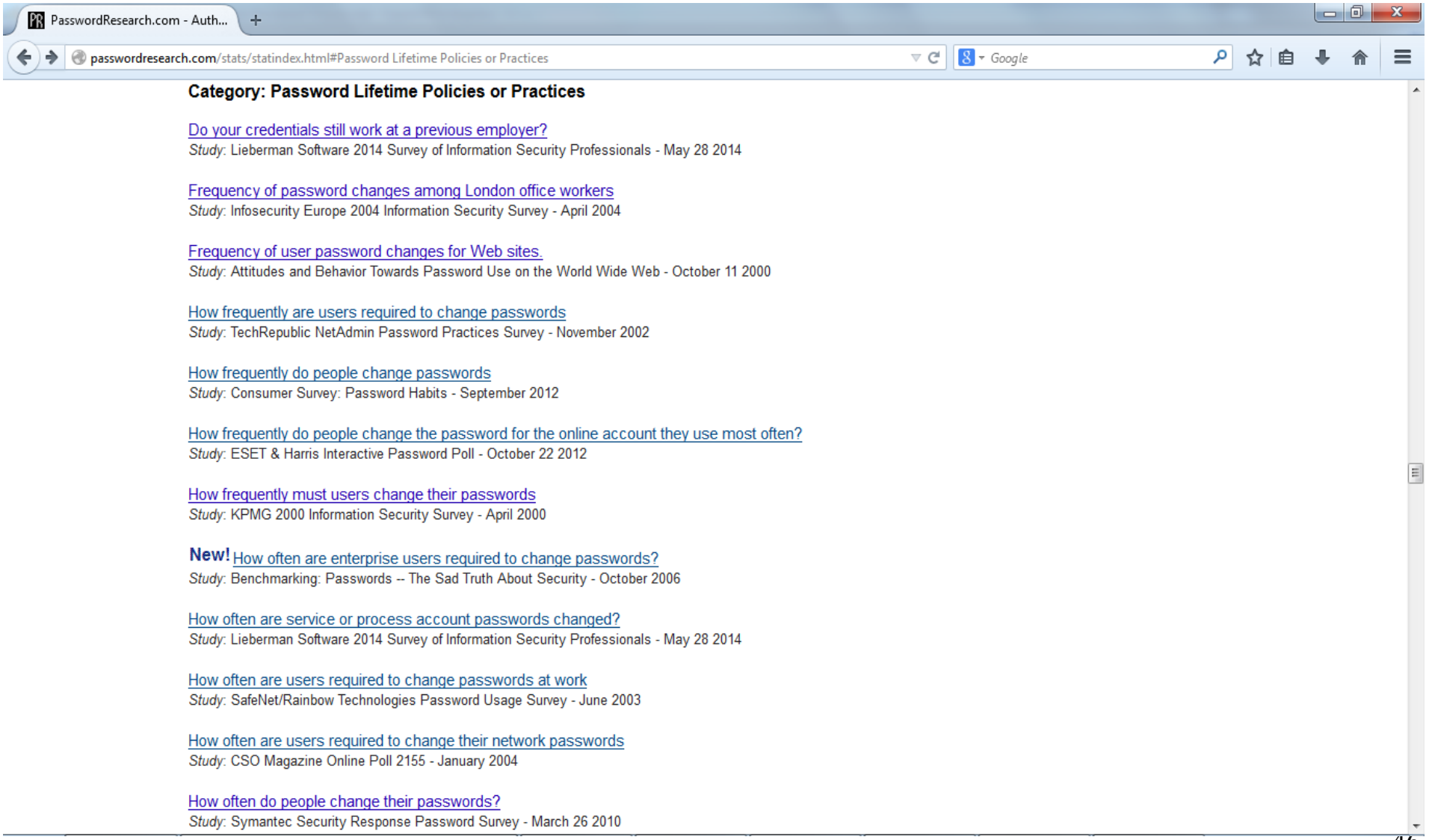
- How do password histories compare in other forced expiration environments?
- Is there an optimal password expiration time frame where forced expiration doesn't result in less secure choices?
- Can user education and awareness make a significant difference in password choice even if expiration is forced?


I'M ONLY 90 DAYS OLD
AND I HAVE TO CHANGE MY PASSWORD ALREADY?!

For More Info

- Bruce K. Marshall
- PasswordResearch.com/Expire.html
- Email: bkmarshall@passwordresearch.com
- @PwdRsch on Twitter

Other Data on Password Expiration



Category: Password Lifetime Policies or Practices

Do your credentials still work at a previous employer?
Study: Lieberman Software 2014 Survey of Information Security Professionals - May 28 2014

Frequency of password changes among London office workers
Study: Infosecurity Europe 2004 Information Security Survey - April 2004

Frequency of user password changes for Web sites.
Study: Attitudes and Behavior Towards Password Use on the World Wide Web - October 11 2000

How frequently are users required to change passwords
Study: TechRepublic NetAdmin Password Practices Survey - November 2002

How frequently do people change passwords
Study: Consumer Survey: Password Habits - September 2012

How frequently do people change the password for the online account they use most often?
Study: ESET & Harris Interactive Password Poll - October 22 2012

How frequently must users change their passwords
Study: KPMG 2000 Information Security Survey - April 2000

New! How often are enterprise users required to change passwords?
Study: Benchmarking: Passwords -- The Sad Truth About Security - October 2006

How often are service or process account passwords changed?
Study: Lieberman Software 2014 Survey of Information Security Professionals - May 28 2014

How often are users required to change passwords at work
Study: SafeNet/Rainbow Technologies Password Usage Survey - June 2003

How often are users required to change their network passwords
Study: CSO Magazine Online Poll 2155 - January 2004

How often do people change their passwords?
Study: Symantec Security Response Password Survey - March 26 2010