Penny-wise and pound-foolish: quantifying the effectiveness of password advice policies

Hazel Murray
The Hamilton Institute & Department of Mathematics and Statistics

Supervisor: Dr. David Malone

Contents

- Collection & categorization of password advice.
- Evaluating the effectiveness of the circulated advice.
- Quantification.
- Example: compare the effectiveness of two password policies.

Collecting advice

Collecting advice

We collected 269 pieces of password advice from 21 different sources.

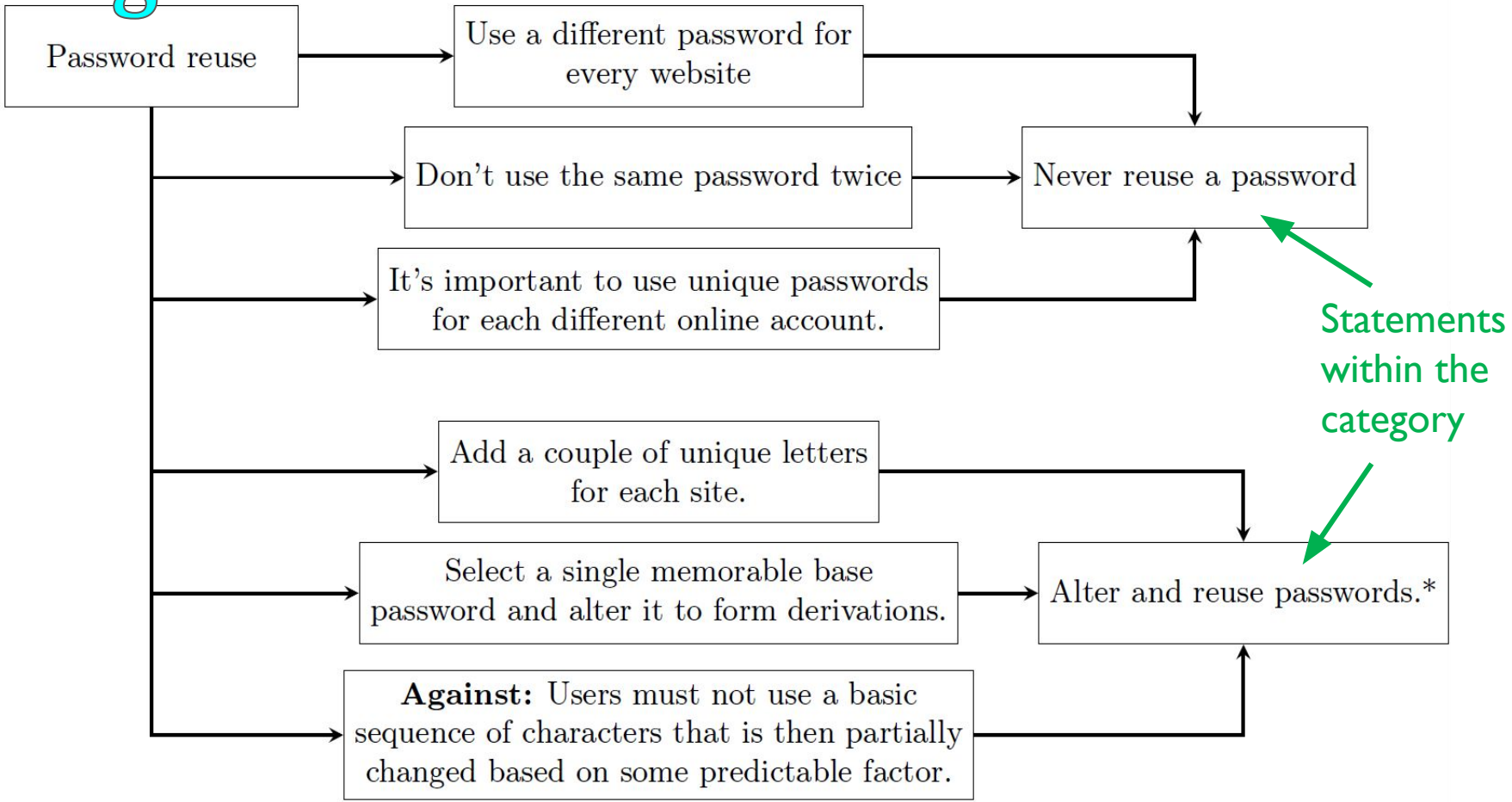
Source		
Multinational companies	e.g. Google	6
Universities	e.g. Boston	6
Security specialists	e.g. NIST	5
General articles	e.g. Get safe online	4

Categorization of advice

Categorization

Users	#	**Organisations**	#
Phrases	32	*Expiry*	27
Composition	28	Length	17
Personal Information	23	Storage	12
Reuse	17	Keeping system safe	8
Personal pwd storage	17	Throttling guesses	8
Backup pwd options	12	Individual accounts	7
Sharing	8	Generated pwds	6
Keeping account safe	8	Transmitting pwds	6
Password managers	5	Admin accounts	5
Username requirements	2	Default passwords	4
Two step verification	2	Shoulder surfing	3
Two factor authentication	1	Access to pwd file	3
		Policies	2
		Input	2
		Network strings	2
		Cracking	1
		Back up work	1
Total	**155**	**Total**	**114**

Categorization



Categorization

Statements for 4 advice categories.

- Reuse
- Phrases
- Composition
- Expiry

Reuse	✘	✓	
Never reuse a password.	5	6	←
Alter and reuse passwords	3	3	←
Don't reuse certain passwords.	0	5	
Phrases	✘	✓	
Don't use patterns.	0	6	
Take initials of a phrase.	0	4	
Don't use published phrases.	1	2	←
Substitute symbols for letters.	1	2	←
Don't use words.	0	16	
Composition	✘	✓	
Must include special characters	5	7	←
Don't repeat characters.	0	3	
Enforce restrictions on characters.	1	12	←
Expiry	✘	✓	
Store history to eliminate reuse.	0	5	
Have a minimum Password Age.	0	1	
Change your password regularly.	4	7	←
Change if suspect compromise.	0	10	

Password reuse

Using a cross-site password guessing algorithm, Das et al. 2014 were able to guess approximately 10% of non-identical password pairs in less than 10 attempts.

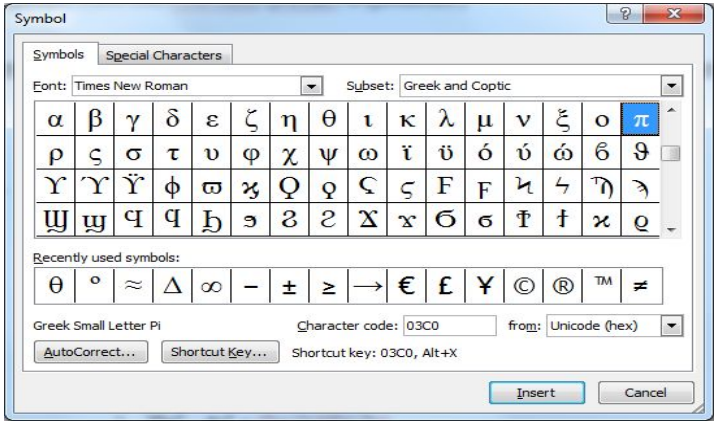
Reuse	✘	✓
Never reuse a password.	5	6
Alter and reuse passwords	3	3
Don't reuse certain passwords.	0	5

Enforcing composition restrictions

Enforce restrictions on characters

The NIST 2017 guidelines was the only advice that disagreed with restrictions on characters.

Composition	✘	✓
Must include special characters	5	7
Don't repeat characters.	0	3
Enforce restrictions on characters.	1	12



Phrases in passwords

Substitute symbols for letters

Warner 2010 showed simple character substitutions are weak.

Don’t use words

Shay et al. 2010 find the use of dictionary words and names are the most common strategies for creating passwords.

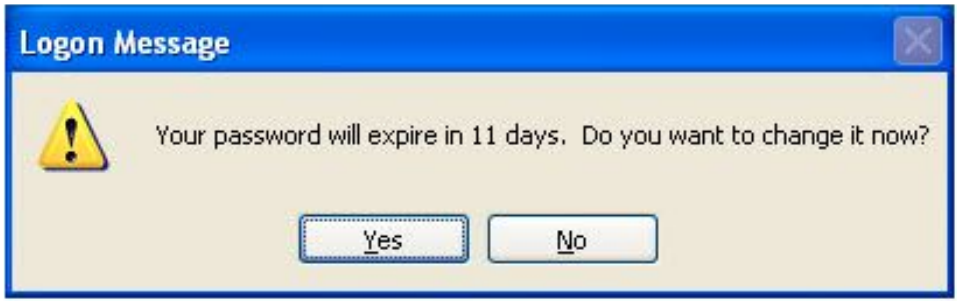
Phrases	✘	✓	
Don’t use patterns.	0	6	
Take initials of a phrase.	0	4	
Don’t use published phrases.	1	2	←
→ Substitute symbols for letters.	1	2	←
→ Don’t use words.	0	16	

Password expiry

Change your password regularly.

Research has show that the security benefits of expiry are minimal. [Zhang et al. 2010, Chiasson et al. 2015]

Expiry	✘	✓
Store history to eliminate reuse.	0	5
Have a minimum Password Age.	0	1
Change your password regularly.	4	7
Change if suspect compromise.	0	10



Murray, H. and Malone, D., 2017, June. Evaluating password advice. In *2017 28th Irish Signals and Systems Conference (ISSC)* (pp. 1-6). IEEE.

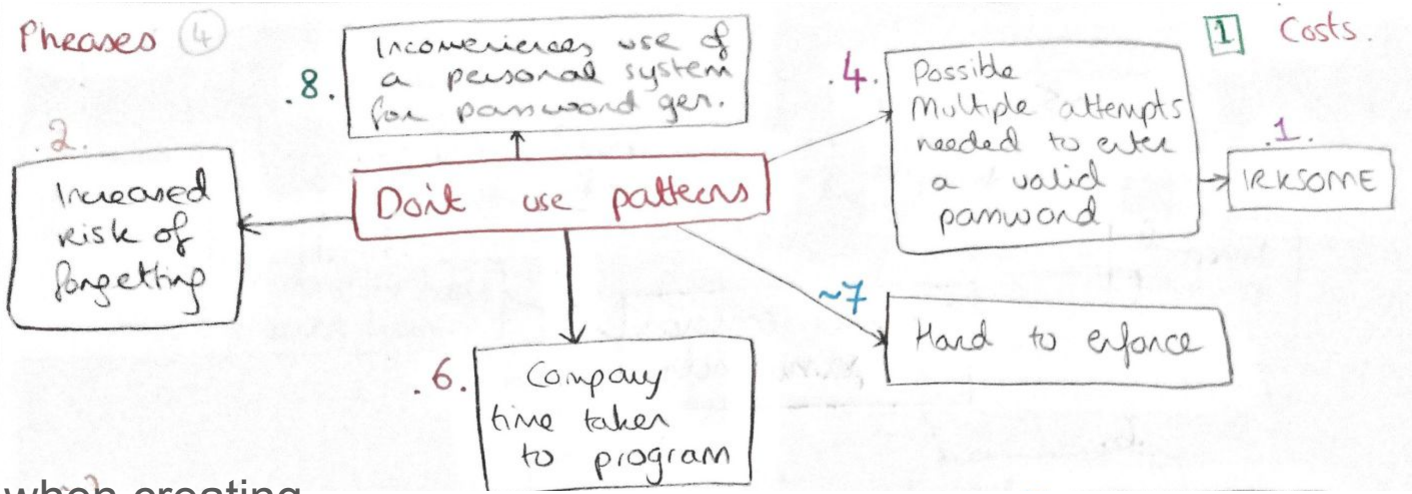
Contents

- Collection & categorization of password advice.
- Evaluating the effectiveness of the circulated advice.
- Quantification.
- Example: compare the effectiveness of two password policies.

Sorting the good advice from the bad?

Costs of password advice

Costs of:



Don't use patterns when creating passwords?

Costs of password advice

Costs of:

Store password history for each user to eliminate reuse.

Costs of password advice

	Costs
1.	Increased risk of forgetting.
2.	Need to pick a new password.
3.	Inconveniences use of a personal system for password generation.
4.	User time or inconvenience.
5.	Organizations' time taken to enforce/program.
6.	Additional resources needed.
7.	Increased computing power needed.

Costs of password advice

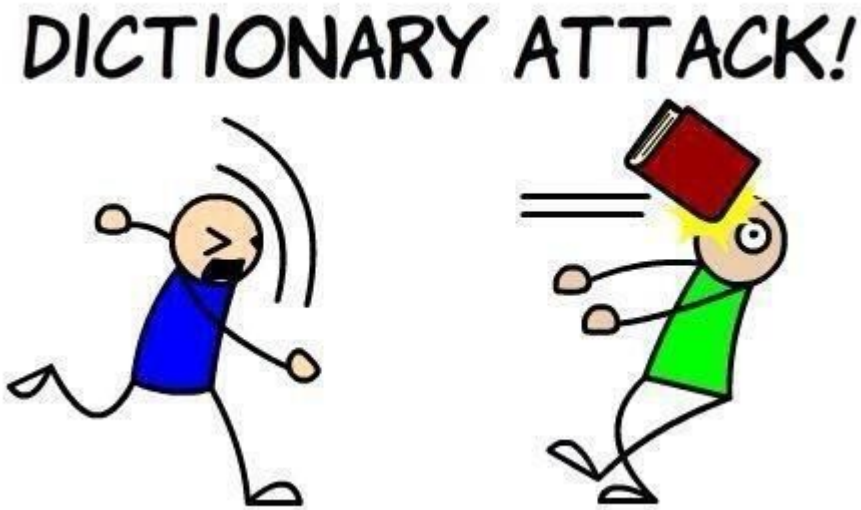
- 205 costs identified, 119 major
- 89% of the major costs were costs that directly affected humans.
- Users experienced significantly more costs than the organization
- Many of the costs to the organization were computing costs.
- Most expensive advice: Use multi-factor authentication.

Other expensive advice. Organizations should:

- Make physical and digital backups.
- Change all default passwords.
- Force users to change their passwords regular
- Regularly apply security patches.

Benefits of password advice

- Guessing attacks
- Phishing
- Eavesdropping
- Side channel
- Theft
- Endpoint compromise



Benefits of password advice

- ✓ Guessing attacks
- ✘ Phishing
- ✘ Eavesdropping
- ✘ Side channel
- \- Theft
- ✘ Endpoint compromise

Attacks protected by:

Never reusing a password,

Benefits of password advice

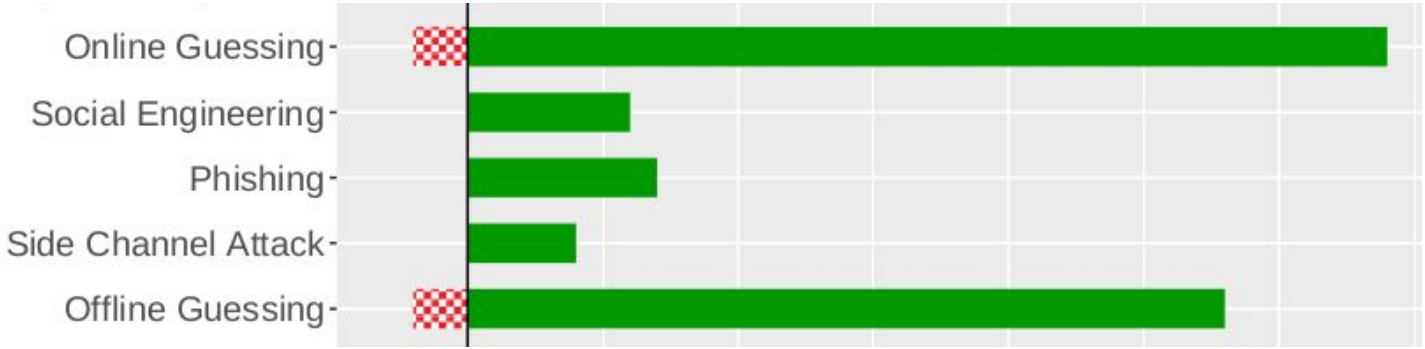
- ✓ Guessing attacks
- ✘ Phishing
- ✘ Eavesdropping
- ✘ Side channel
- ⬆️ Theft
- ✘ Endpoint compromise

Attacks protected by:

Store password history for each user to eliminate reuse.

Benefits of password advice

- Identified 201 benefits, 124 were major.
- 7 pieces of advice resulted in increased chance of compromise
- Biggest negative impact on security: Enforce maximum password length
- Advice offering the most protection from attack: Set up one account per user



Costs versus Benefits

Good usable security advice

- Email up-to-date and secure
- Do not store hints
- Create long random passwords when using a password manager
- Don't send password by email
- Don't give passwords over the phone
- One account per user
- Don't perform truncation
- Encrypt files
- Don't transmit in cleartext
- Request over a protected channel

Costs versus Benefits

Bad advice

- Security answers difficult to guess
- Enforce restrictions on characters
- Manually type URLs
- Enforce restrictions on characters used in username
- Enforce maximum length (<40)
- Don't allow users to paste passwords

Contents

- Collection & categorization of password advice.
- Evaluating the effectiveness of the circulated advice.
- Quantification.
- Example: compare the effectiveness of two password policies.

VALUE OF A PASSWORD POLICY=

BENEFITS of the policy – COSTS of the policy

Benefits of a password policy

E[Benefits] = E[Loss without policy] - E[Loss with policy]

- What is the **probability of compromise** with and without the security policy?
- What is the **loss as a result of a compromise**?

Probability of compromise

- Guessing attacks
- Phishing
- Eavesdropping
- Side channel
- Theft
- Endpoint compromise

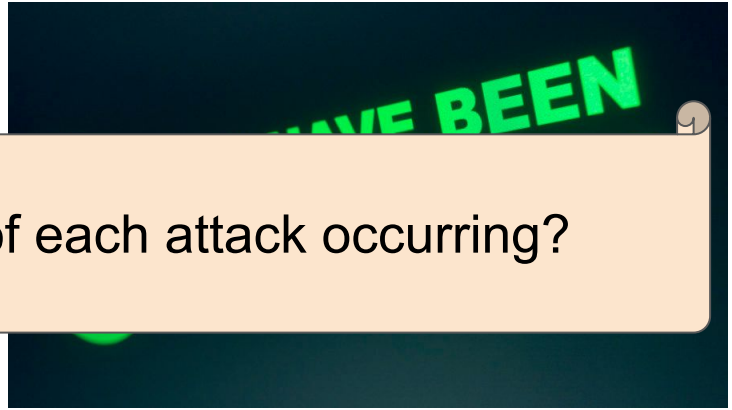
$$\text{Probability of compromise} = 1 - \prod(1 - p_a)$$

Probability of compromise

- Guessing attacks
- Phishi
- Eaves
- Side c
- Theft
- Endpoint compromise

Difficult 1

How to find the probability of each attack occurring?



$$\text{Probability of compromise} = 1 - \prod(1-p_a)$$

How to find the probability of each attack occurring?

When there is no policy in place the probability an eavesdropping attack is successful is:

P[eavesdropping | no policy] = P[network eavesdropping breach] + P[keylogger breach] + P[physical surveillance breach]

But if passwords are encrypted before transmission. Then the probability of an eavesdropping attack is:

P[eavesdropping | encrypted] = P[physical surveillance] +P[keylogger breach]

Murray, H. and Malone, D., 2018, August. Exploring the Impact of Password Dataset Distribution on Guessing. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)* (pp. 1-8). IEEE.

How to find the probability of each attack occurring?

When there is no policy in place the probability an eavesdropping attack is successf

P[no policy] = P[network eavesdropping breach] + P[keylogger br al surveillance breach]

Difficult 2

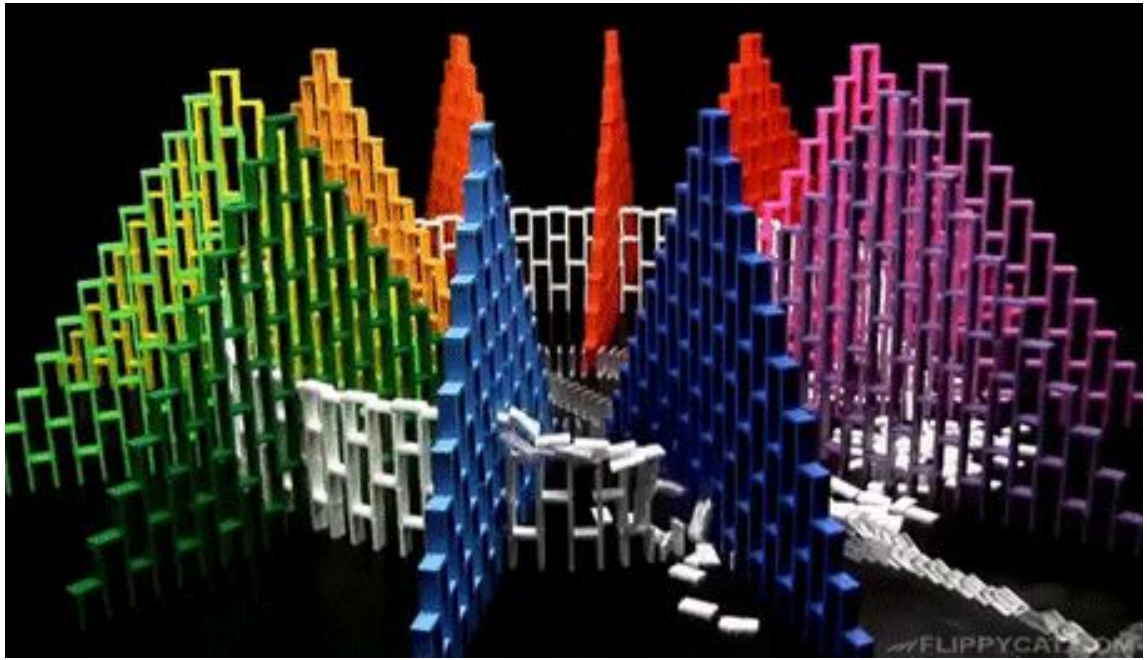
But if pas n eavesdro

P[eavesdropping | encrypted] = P[physical surveillance] +P[keylogger breach]

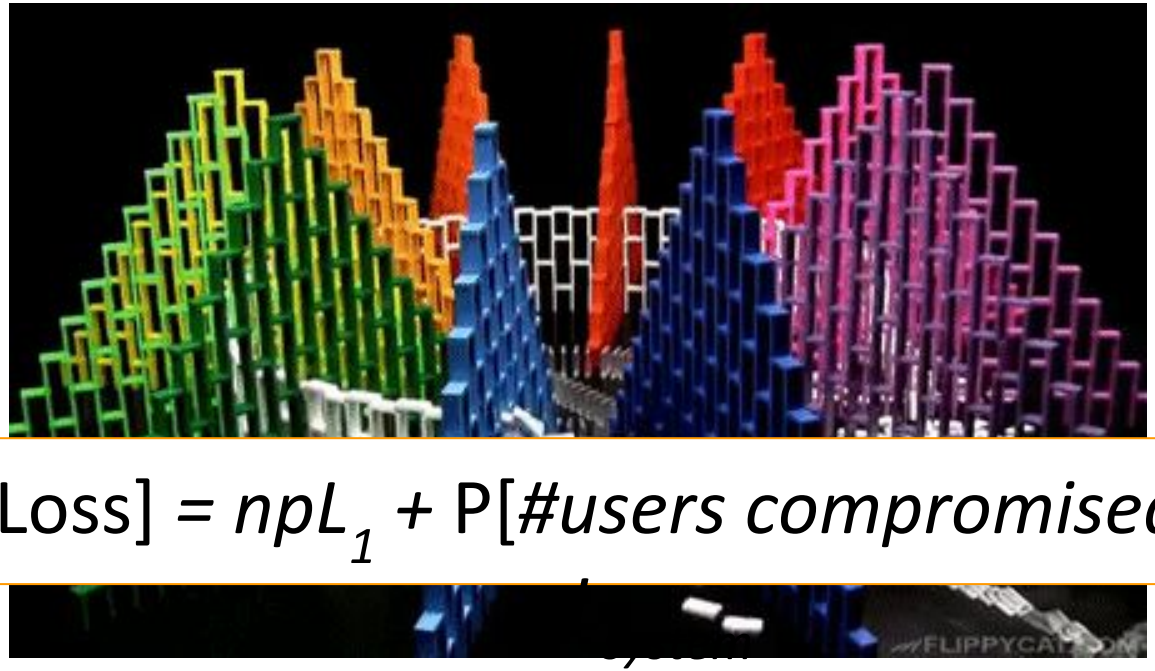
We have no idea what security policies the organisations compromised had in place.

Murray, H. and Malone, D., 2018, August. Exploring the Impact of Password Dataset Distribution on Guessing. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)* (pp. 1-8). IEEE.

Loss as a result of a compromise



Loss as a result of a compromise



$$E[\text{Loss}] = npL_1 + P[\#\text{users compromised} > \alpha.n]$$

n = number of users; p = probability 1 user is compromised;

L_1 =Loss from one user compromise; L_{system} = Loss if system is compromise

Costs of a password policy

	Costs
1.	Increased risk of forgetting.
2.	Need to pick a new password.
3.	Inconveniences use of a personal system for password generation.
4.	User time or inconvenience.
5.	Organizations' time taken to enforce/program.
6.	Additional resources needed.
7.	Increased computing power needed.

c_1 = Cost if user forgets password =

(Time taken for administrator to reset the passwords)(€Administrator wages)

\+ (Time that user is locked out of their account)(€User wages)(U)

\+ P[user abandons the site] (€Profit per user)

Costs of a password policy

	Costs
1.	Increased risk of forgetting.
2.	Need to pick a new password.
3.	Inconveniences use of a personal system for password generation.
4.	User time or inconvenience.
5.	Organizations' time taken to enforce/program.
6.	Additional resources needed.

$$E[\text{Costs}] = \sum_j \sum_i (p_i c_i r_i)$$

c_1 Cost if user forgets password

(Time taken for administrator to reset the passwords)(€Administrator wages)

\+ (Time that user is locked out of their account)(€User wages)(U)

\+ P[user abandons the site] (€Profit per user)

Contents

- Collection & categorization of password advice.
- Evaluating the effectiveness of the circulated advice.
- Quantification.
- Example: compare the effectiveness of two password policies.

Example password policy 1

NIST 2017 Password policy (Level 1)

- Length >8
- Blacklist compromised passwords
- Limit consecutive failed login attempts to 100
- Hash and Salt passwords
- Send messages over a protected channel

Example password policy 2

NIST 2003 Password policy (Level 1)

- No composition requirements
- Lock the password for 1 minute after 3 incorrect guesses.
- Passwords stored using reversible encryption

Constants

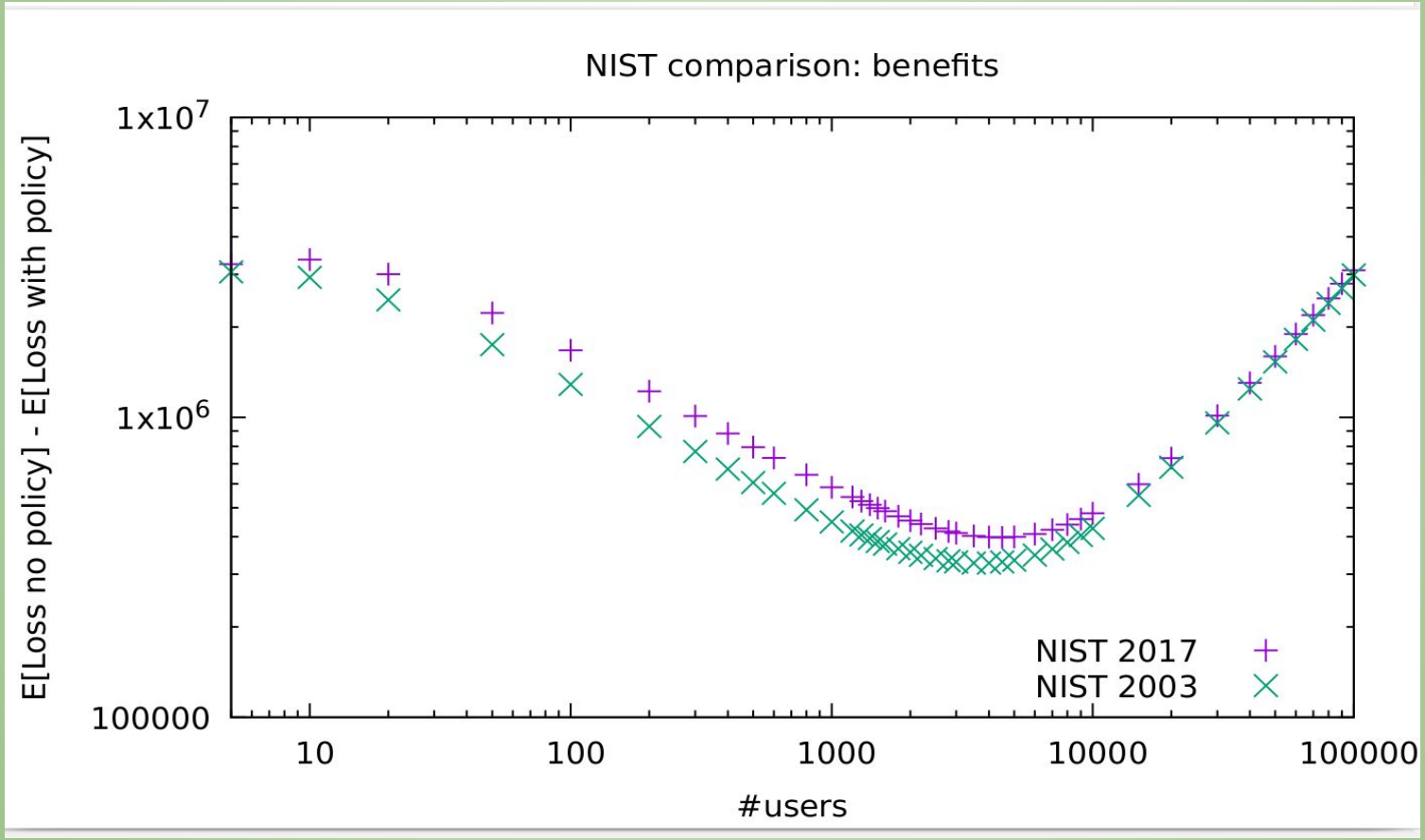
L1 = 166

Lsytsem = 10,000,000

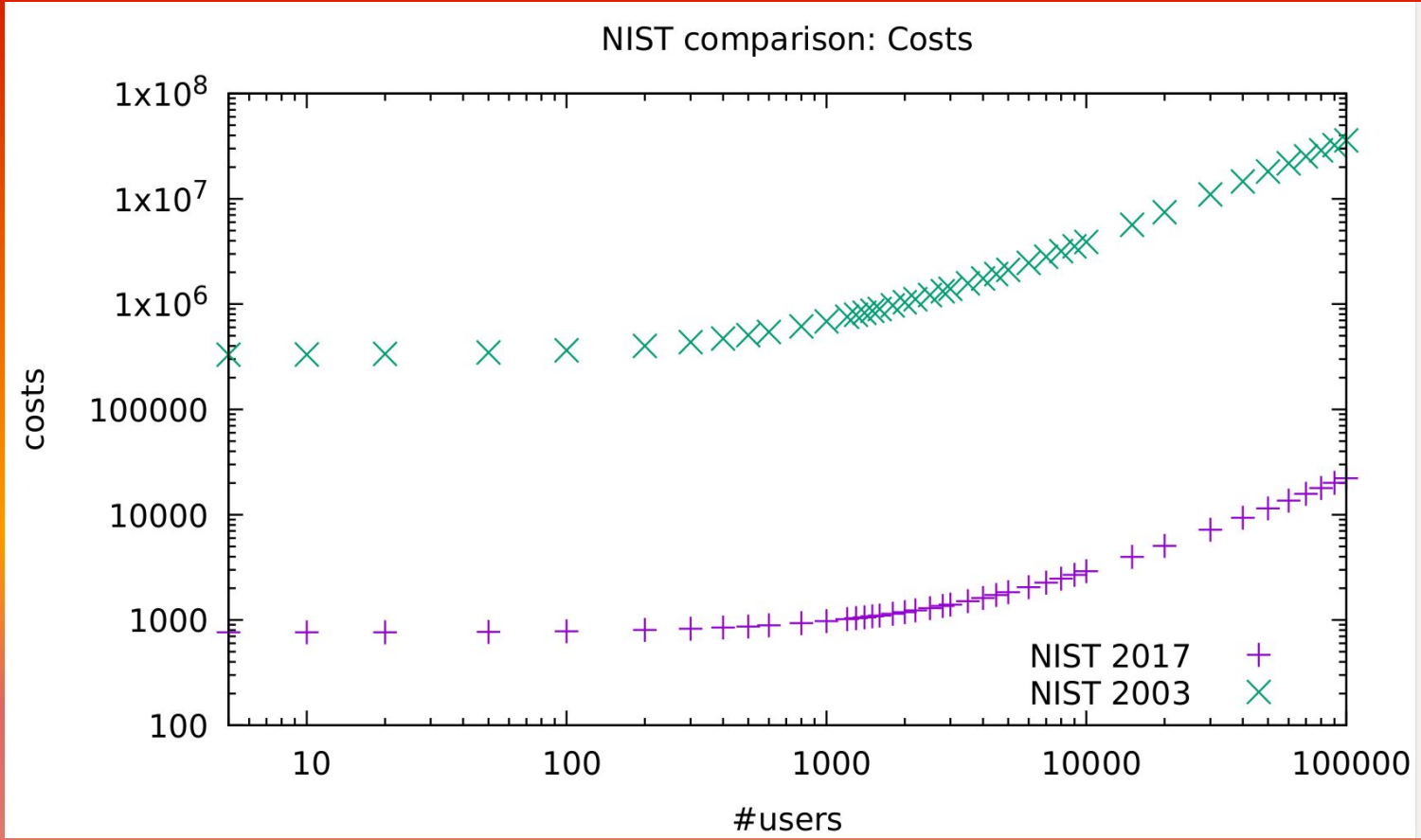
α =0.5

U =1

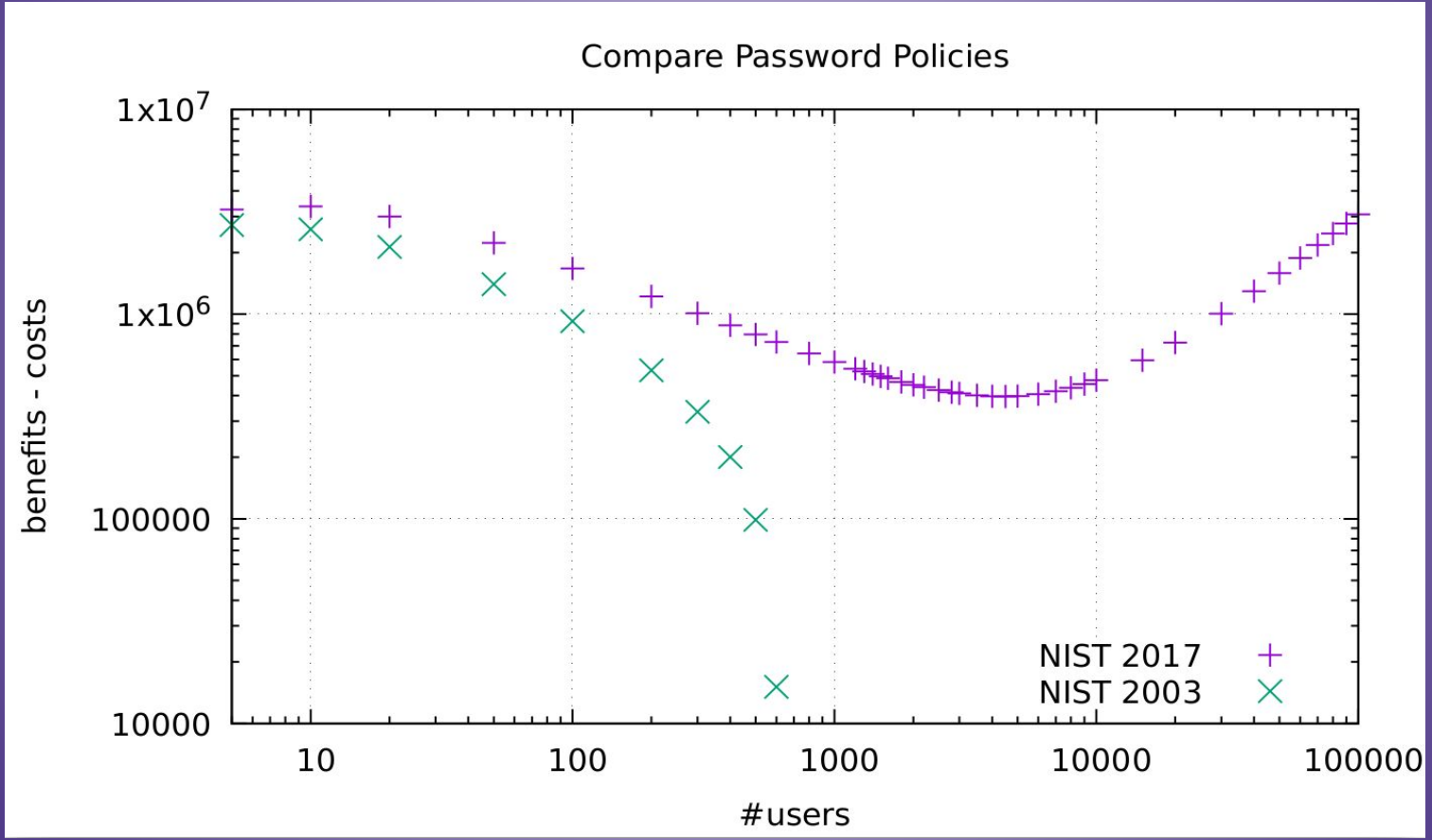
Benefits


NIST comparison: benefits
E[Loss no policy] - E[Loss with policy]
1x10^7
1x10^6
100000
10
100
1000
10000
100000
#users
NIST 2017
NIST 2003

Costs


NIST comparison: Costs
costs
#users
1x10^8
1x10^7
1x10^6
100000
10000
1000
100
10
100
1000
10000
100000
NIST 2017
NIST 2003

Compare password policies



Conclusions

Just like everything, before implementing authentication policies, both the costs and benefits need to be weighed.

It is the human users who suffer when the costs of a policy are high.

Sometimes organizations focus all their effort on one attack type forgetting about the whole attack spectrum.

Thank you.