A penny for your password

Hazel Murray, David Malone

Password advice is constantly circulated. Yet there is little research determining what advice is good and what advice is bad. Herley (2009) argues that users' rejection of security advice is rational from an economic perspective. We aim to develop a framework for identifying whether the benefits of password advice outweigh the cost of enforcing the advice.

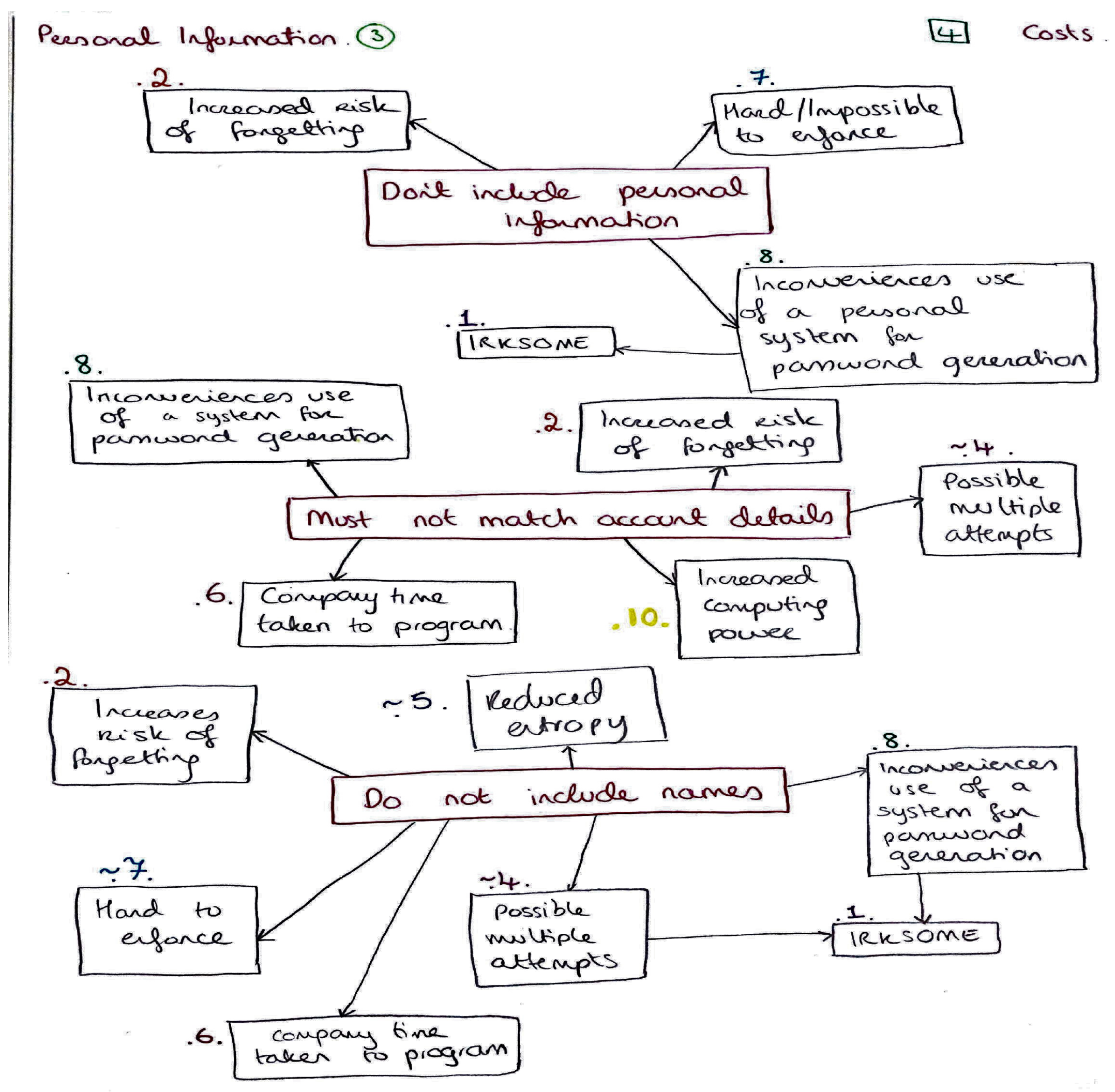
Previous work

In our previous paper "Evaluating Password Advice" we collected password advice and found that the advice distributed by one organization can directly contradict advice given by another.

We aim to develop a framework to determine what password advice is good and what advice is bad.

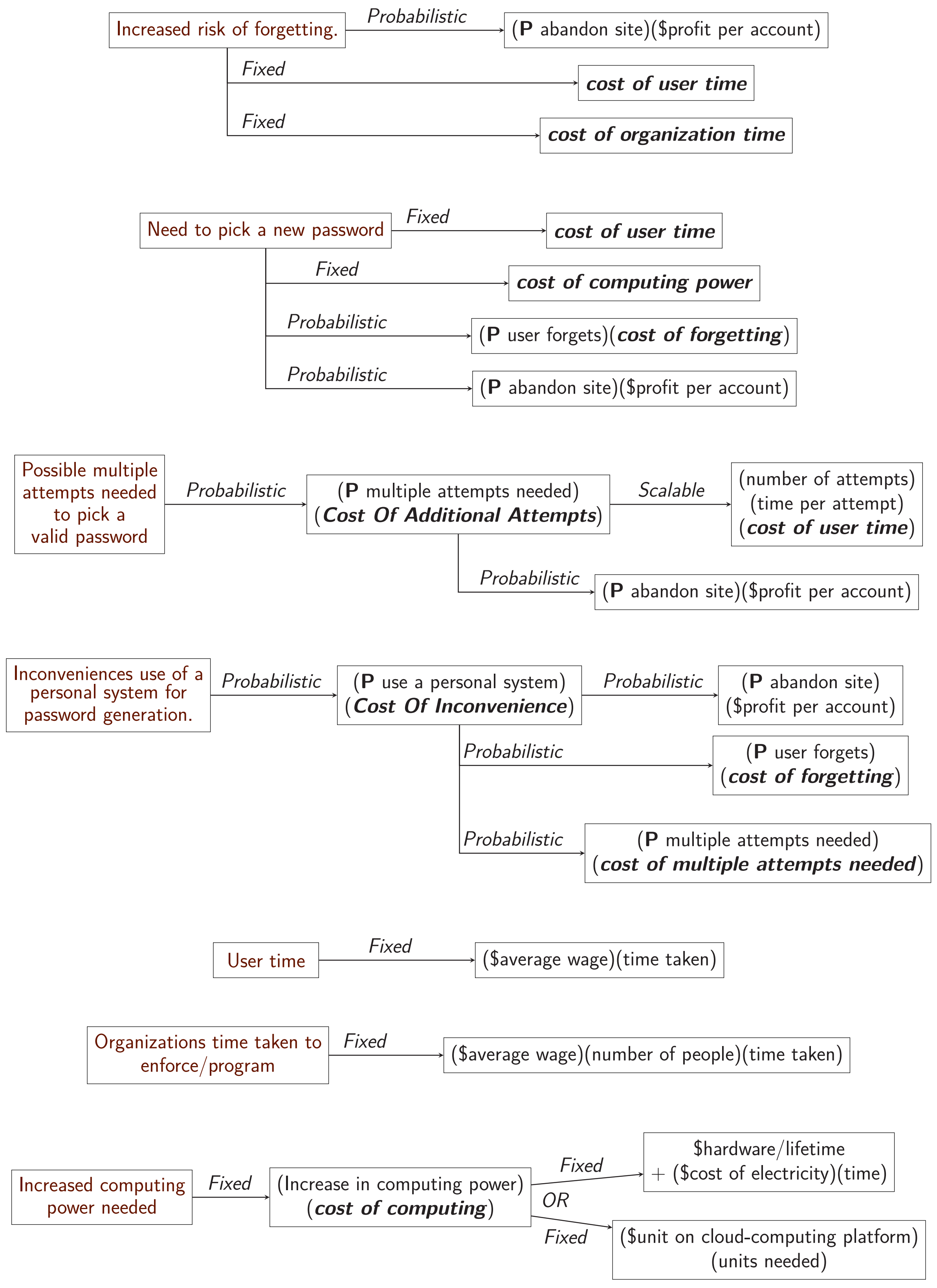
Identifying Costs

For each type of password advice we brainstormed to find the associated costs.


Personal Information. ③
4 Costs.
.2.
Increased risk of forgetting
.7.
Hard/Impossible to enforce
Don't include personal information
.8.
Inconveniences use of a personal system for password generation
.1.
IRKSOME
.8.
Inconveniences use of a system for password generation
.2.
Increased risk of forgetting
~4.
Possible multiple attempts
Must not match account details
.6.
Company time taken to program
.10.
Increased computing power
.2.
Increases risk of forgetting
~5.
Reduced entropy
Do not include names
.8.
Inconveniences use of a system for password generation
~7.
Hard to enforce
~4.
Possible multiple attempts
.1.
IRKSOME
.6.
company time taken to program

	Categories of costs
1.	Increased risk of forgetting.
2.	Need to pick a new password.
3.	Possible multiple attempts needed to enter a valid password.
4.	Inconveniences use of a personal system for password generation.
5.	User time taken.
6.	Reduced "entropy".
7.	Organizations' time taken to enforce/program.
8.	Impossible/hard to enforce.
9.	Creates an additional security hole.
10.	Increased computing power needed.

Methods for Quantifying Costs



Increased risk of forgetting. —*Probabilistic*→ (**P** abandon site)($profit per account)

Increased risk of forgetting. —*Fixed*→ ***cost of user time***

Increased risk of forgetting. —*Fixed*→ ***cost of organization time***

Need to pick a new password —*Fixed*→ ***cost of user time***

Need to pick a new password —*Fixed*→ ***cost of computing power***

Need to pick a new password —*Probabilistic*→ (**P** user forgets)(***cost of forgetting***)

Need to pick a new password —*Probabilistic*→ (**P** abandon site)($profit per account)

Possible multiple attempts needed to pick a valid password —*Probabilistic*→ (**P** multiple attempts needed)(***Cost Of Additional Attempts***)

(**P** multiple attempts needed)(***Cost Of Additional Attempts***) —*Scalable*→ (number of attempts)(time per attempt)(***cost of user time***)

(**P** multiple attempts needed)(***Cost Of Additional Attempts***) —*Probabilistic*→ (**P** abandon site)($profit per account)

Inconveniences use of a personal system for password generation. —*Probabilistic*→ (**P** use a personal system)(***Cost Of Inconvenience***)

(**P** use a personal system)(***Cost Of Inconvenience***) —*Probabilistic*→ (**P** abandon site)($profit per account)

(**P** use a personal system)(***Cost Of Inconvenience***) —*Probabilistic*→ (**P** user forgets)(***cost of forgetting***)

(**P** use a personal system)(***Cost Of Inconvenience***) —*Probabilistic*→ (**P** multiple attempts needed)(***cost of multiple attempts needed***)

User time —*Fixed*→ ($average wage)(time taken)

Organizations time taken to enforce/program —*Fixed*→ ($average wage)(number of people)(time taken)

Increased computing power needed —*Fixed*→ (Increase in computing power)(***cost of computing***)

(Increase in computing power)(***cost of computing***) —*Fixed*→ $hardware/lifetime + ($cost of electricity)(time)

OR

(Increase in computing power)(***cost of computing***) —*Fixed*→ ($unit on cloud-computing platform)(units needed)

Quantifying benefits

Zhang et al. (2016) identified four key threats to passwords:

- Password capture,
- Online password guessing,
- Offline password guessing,
- Targeted password guessing.

To calculate the benefits we need to determine the frequency of each attack, the success rate for each attack and the reduction in the probability of the attack's success as a result of the password advice.

$$\textbf{Costs} = N_1\left[\sum \textit{fixed} + \sum \textit{probabilistic costs}\right]$$

where N_1 is the number of times the costs occur over the given time period.

$$\textbf{Benefits} = \textit{Value of Protected}\cdot$$

$$\left[\underbrace{\sum N_2 \cdot \mathbf{P}_{\textit{success}\,1}}_{\textit{once-off-attacks}} + \underbrace{\sum 1 - e^{-t\lambda \mathbf{P}_{\textit{success}\,2}}}_{\textit{scalable-attacks}}\right]$$

where N_2 is a number of attacks, λ is the number of scalable attacks per second, and t is the time period.

Acknowledgments

This publication has emanated from research supported in part by a research grant from Science Foundation Ireland (SFI) and is co-funded under the European Regional Development Fund under Grant Number 13/RC/2077. This research is supported by the Irish Research Council Postgraduate Scholarship 2017.

Feedback: This is the very beginning off our research into quantifying the costs and benefits of password advice. We would appreciate any input and advice offered.