Password Portfolios and the Finite-Effort User:

Sustainably Managing Large Numbers of Accounts

Dinei Florencio, Cormac Herley and Paul C. van Oorschot

Microsoft Research and Carleton University

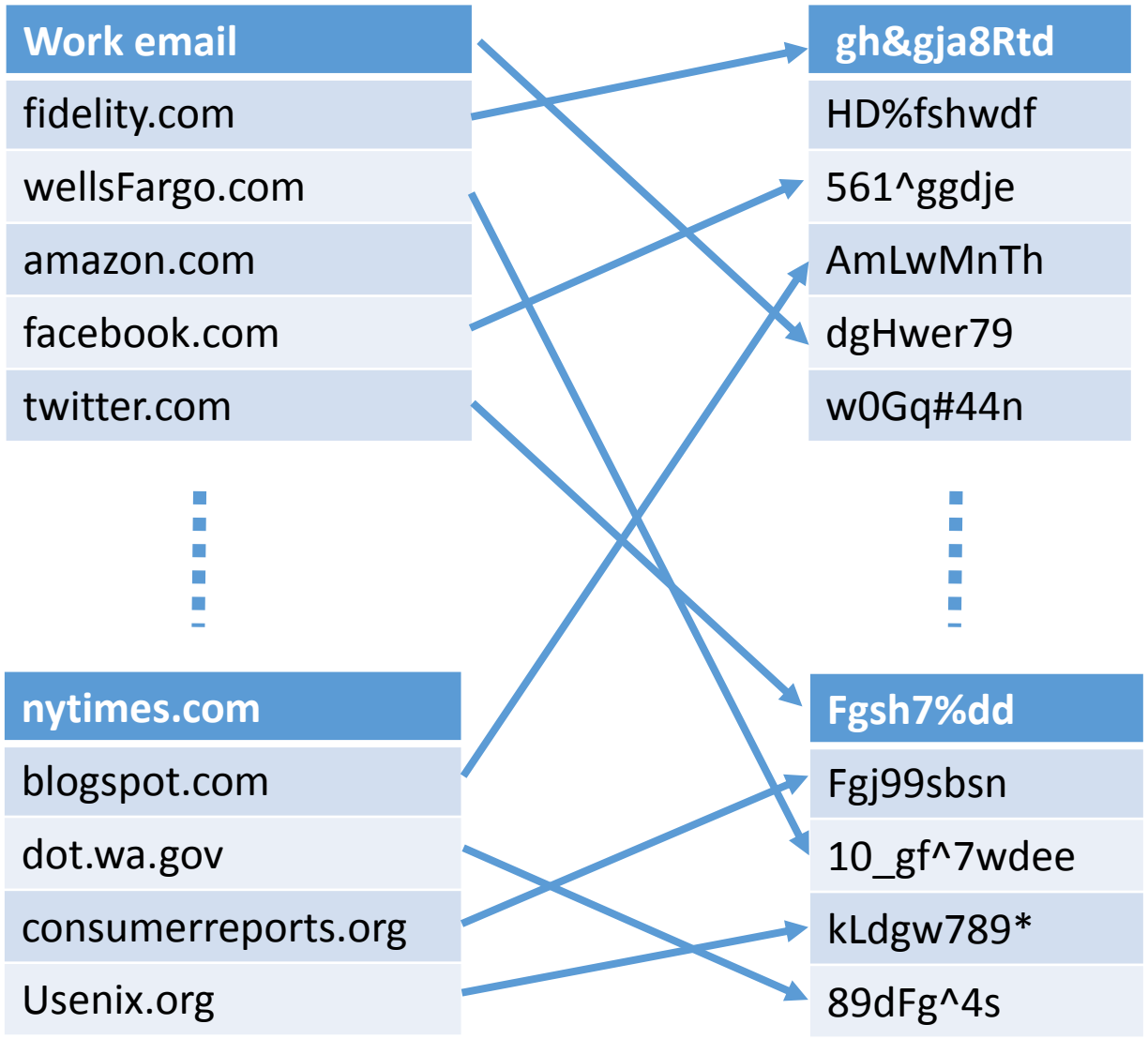
Choosing a password

Everyone knows

A1: Passwords should be random and strong

A2: Passwords should not be re-used across accounts

But no-one does.



lg(N!) + N·lg(S)

Portfolio of N random, unique Passwords lg(S) each

Must remember:

- N passwords = N·lg(S)
- NxN pwd-to-acct assignment = lg(N!)

E(N) = N·lg(S) + lg(N!)

Remembering N random passwords

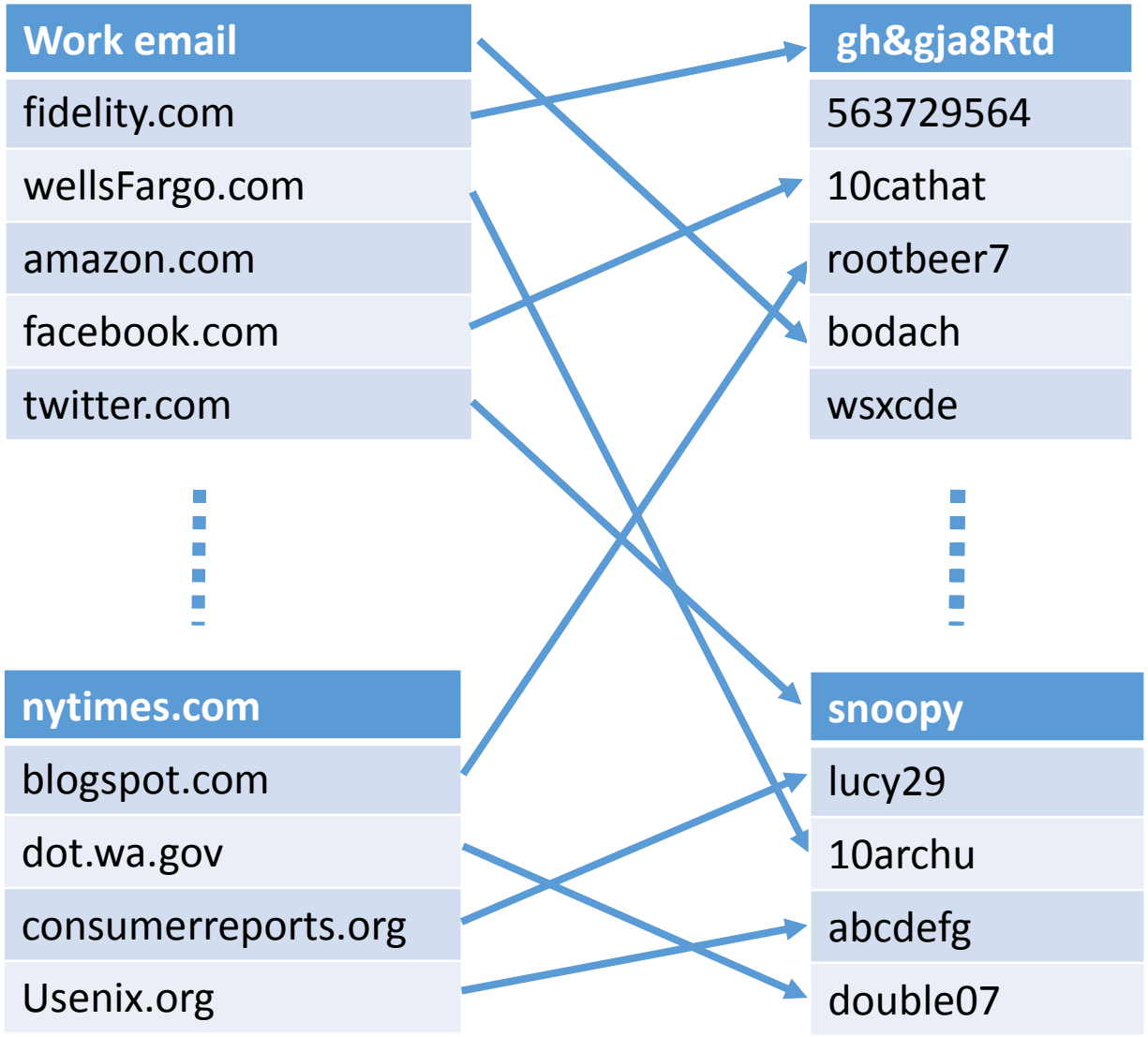
$$E(N) = N \cdot \lg(S) + \lg(N!)$$

E.g. N=100 accts, lg(s)=40

$$E(100) = 4000 + 524 = 4524 \text{ bits}$$

Depends how remember passwords

Random bits



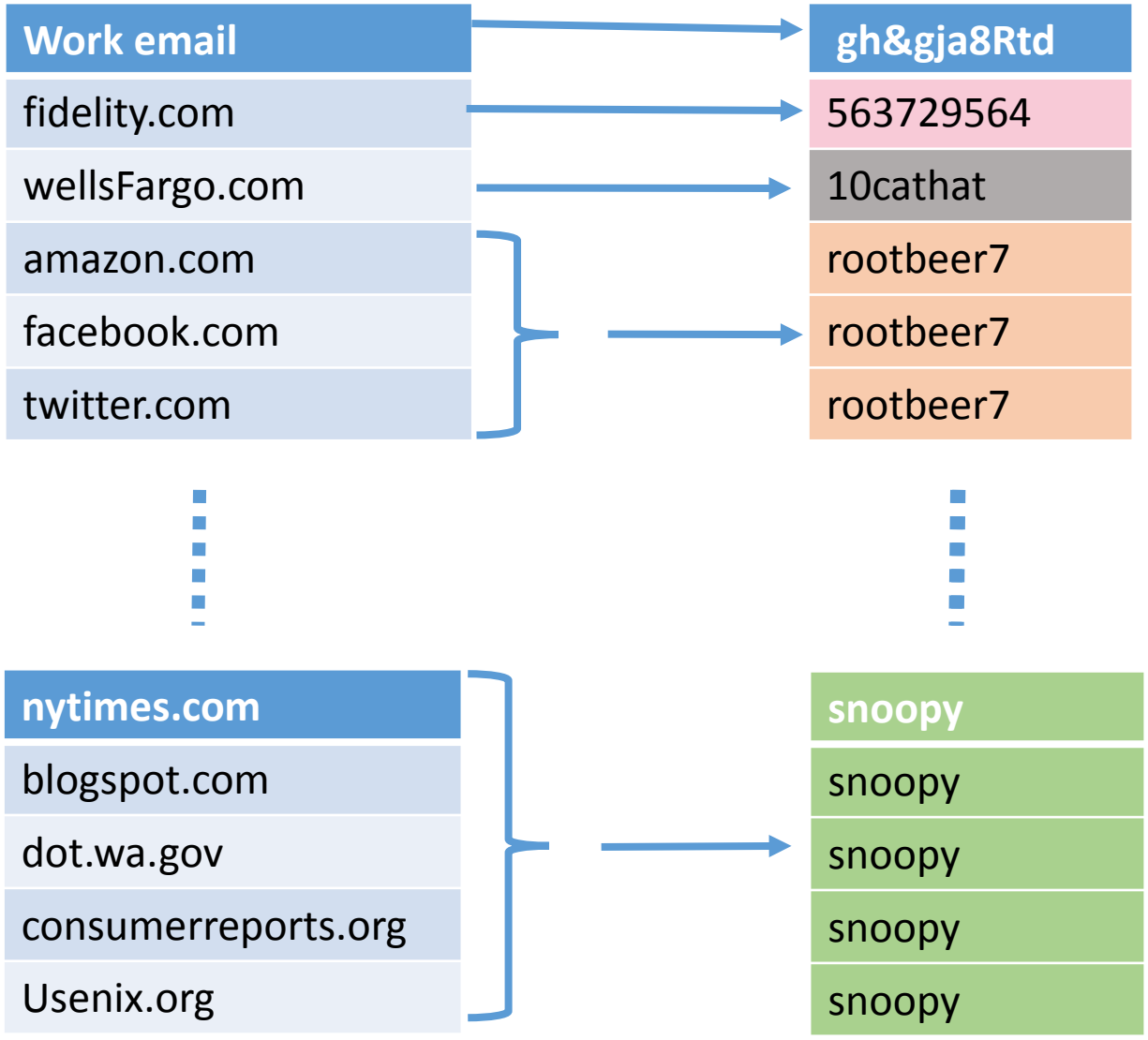
Reducing the burden

Coping strategy:

- Weaker passwords: reduce lg(S)

$$E(N) = 100 \cdot \lg(S) + 524$$

Way too high, even if lg(S)=0!!!



Reducing the burden

Group and re-use

Effort for N accounts in G groups: $E_G(N)$

$$E_G(N) \approx G \cdot \lg(S) + N \cdot \lg(G)$$

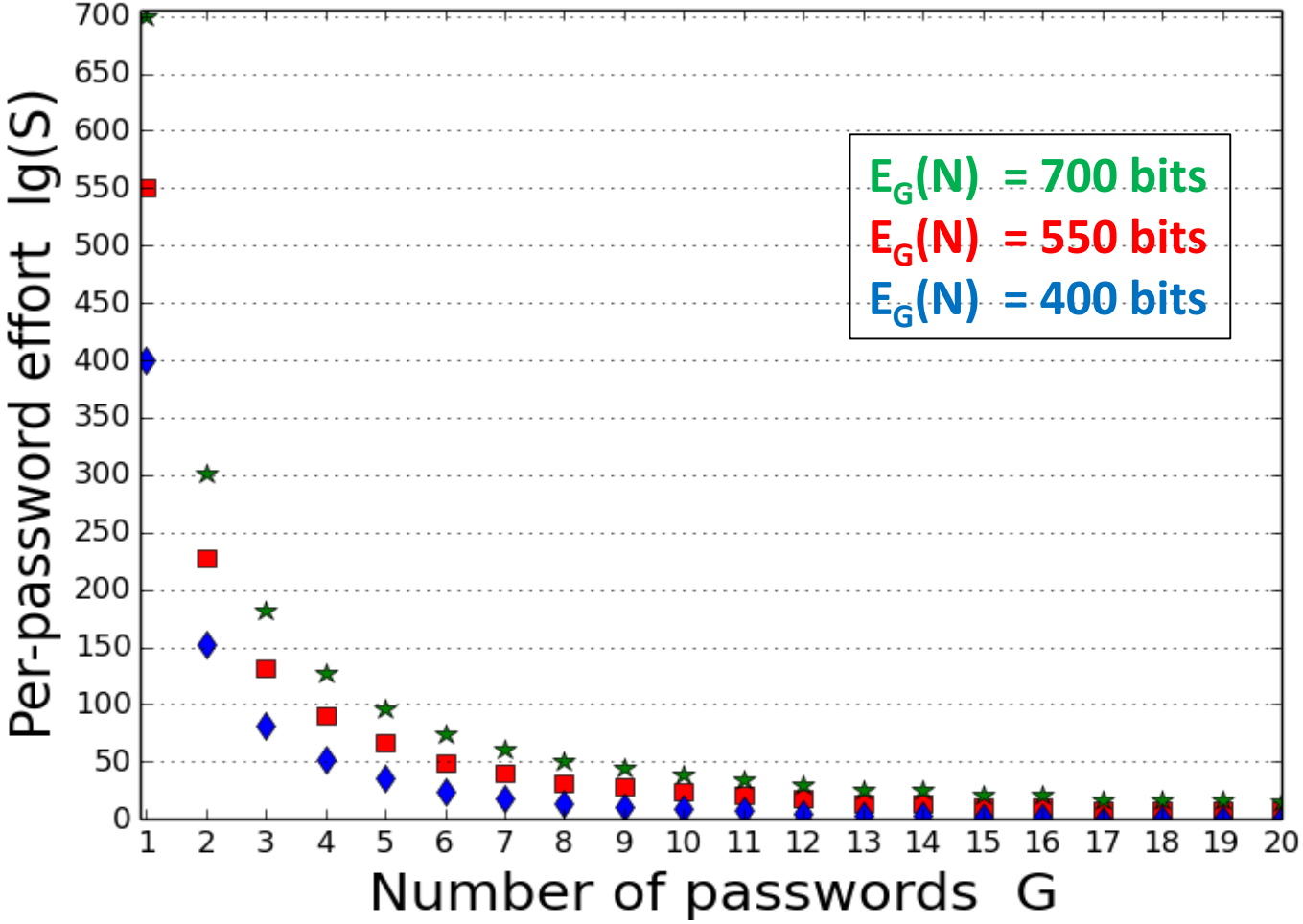
$$\Rightarrow \qquad \lg(S) \approx \frac{(E_G(N) - N \cdot \lg(G))}{G}$$

Reciprocal reln: tradeoff between strength and avoiding re-use (i.e. lg(S) and G)

N = #accts
G = #unique pwds
lg(S) = pwd strength

Many ways to organize portfolio

$$\lg(S) \approx (E_G(N) - N \cdot \lg(S))/G$$



Fixed effort:

- lg(S) α 1/G
- Stronger pwd => more re-use

Doubling #pwds more than halves pwd strength.

“What was the question again?”

Q: Minimize portfolio ***expected loss***?

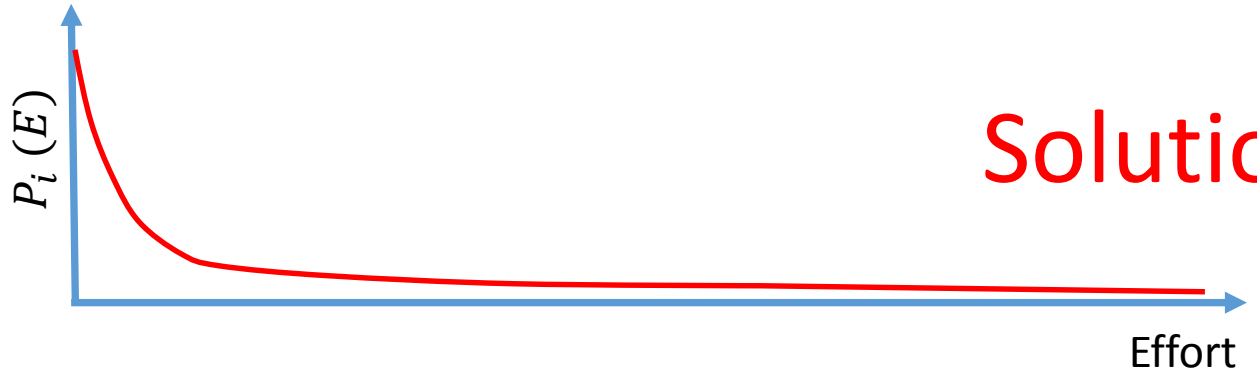
$$L = \sum_{i=1}^{N} P_i\,(E)\,L_i$$

$P_i(E)$ = Pr. Compromise
L_i = i-th value

Set $dL/dE = 0$: (If all accts independent)

$$\Rightarrow \quad \frac{dP_i\,(E_i)}{dE_i} = 0 \qquad \text{for } i=1,2,3,\ldots, N$$

Probability of harm decreases with effort.



Solution: Effort → ∞

Users also care about effort!!!!!

Q: Minimize ***expected loss + effort***?

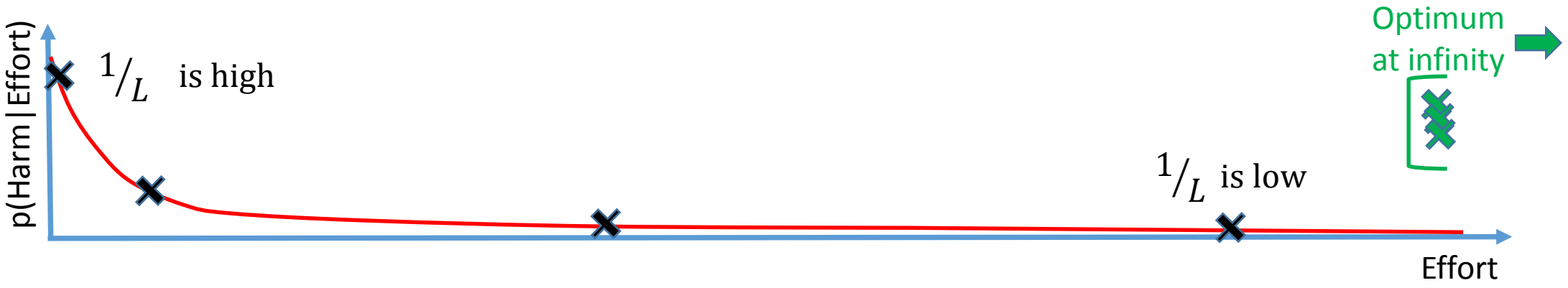
$$L + E = \sum_{i=1}^{N} (P_i\,(E_i)\,L_i + E_i)$$

Optimality: set $d(L+E)/dE = 0$ (If all accts independent)

$$\Rightarrow \qquad \frac{dP_i\,(E_i)}{dE_i} = {}^{-1}\!/_{L_i} \qquad \text{for } i=1,2,3,\ldots,\ N$$

Difference the objective function makes:

- Minimize: *L* (all passwords as strong as possible)
- Minimize: *L + E* (effort depends on dP/dE and L)



Are we done? Not quite…….
Re-use Complicates things

Risk is not:

- Independent across accounts
- Dependent only on strength

- Risk to i-th acct also depends on
  - Effort for other accts that share the password
  - Effort to protect from keyloggers, malware

Without this simplification: set of N non-linear eqns

Segmentation: Attack Classes I, II, III

	Class I	Class II	Class III
	Full	Group	Single acct
Attack	Keyloggers	Password guessing, phishing; server DB leaks	Session-hijacking, XSS
Effort addressing	AV, updates, PC hygiene	Strong passwords, avoid re-use, avoid phishing sites.	

Realistic Model, Minimize L+E

Expected Portfolio loss

$$L = P^{I}\sum_{i=1}^{N} L_i + \sum_{J=1}^{G}\left(\sum_{i\in\mathscr{A}_J} P_i^{II}\right)\left(\sum_{i\in\mathscr{A}_J} L_i\right) + \sum_{i=1}^{N} P_i^{III} L_i$$

L+E minimized when:

$$\frac{\partial(L+E)}{\partial E^{I}} = \frac{\partial(L+E)}{\partial E^{II}} = \frac{\partial(L+E)}{\partial E^{III}} = 0$$

Which gives…….

$$\left(\sum_{i=1}^{N} L_i\right)\frac{\partial P^I}{\partial E^I} = -1$$

$$L_J \cdot \frac{\partial P_J}{\partial E_J} = -1, J = 1 \cdots G$$

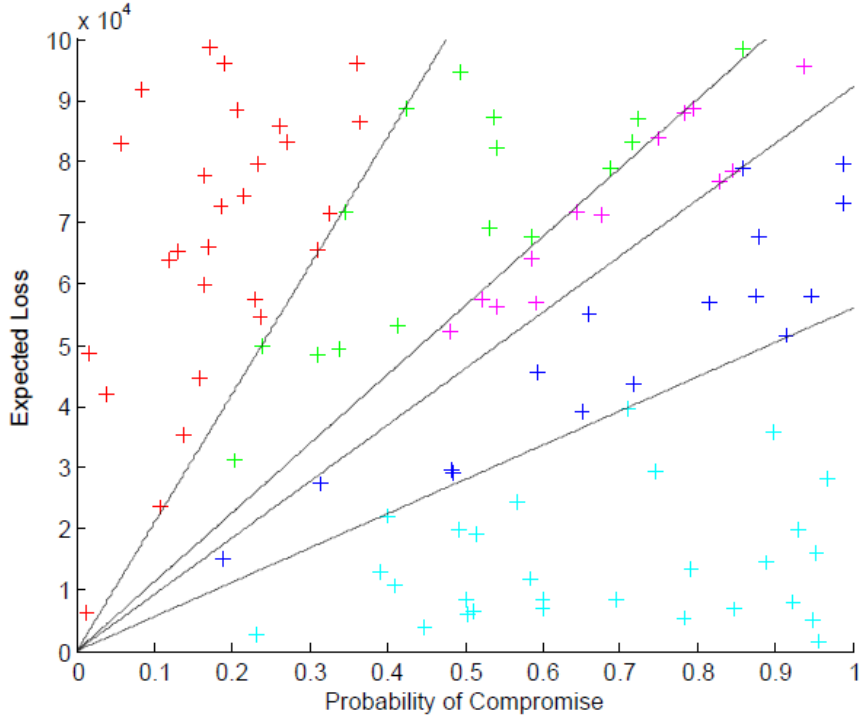
$$L_i \cdot \frac{\partial P_i^{III}}{\partial E_i^{III}} = -1, i = 1 \cdots N.$$

…which is a set of linear equations

Criteria for optimality now give:

Decision boundaries between groups J, K

$$L = \left(\frac{L_J - L_K}{P_K - P_J} \right) P$$



Groups have similar weighted loss

$$P_J L_J \approx P_K L_K$$

Conclusion/Take-away points

- Random and unique passwords infeasible for large portfolios
- User interest is to minimize L+E, rather than L, over the portfolio.
- Realistic analysis must include attacks that cover:
  - I: all accts,
  - II: password sharing groups,
  - III: single accounts.

Conclusions cntd.

- A strategy that rules out re-use is sub-optimal
- A strategy that rules out weak passwords is sub-optimal
- Group like with like: e.g.
  - High-value, low probability of compromise
  - Low-value, high probability of compromise