

Naturally Rehearsing Passwords

(to appear at ASIACRYPT 2013)

Jeremiah Blocki



Manuel Blum



Anupam Datta

Person Action Object (PAO) Stories



Person Action Object (PAO) Stories



Person Action Object (PAO) Stories



Person	Manuel Blum
Action	torturing
Object	lion

PAO Story #2



PAO Story #2

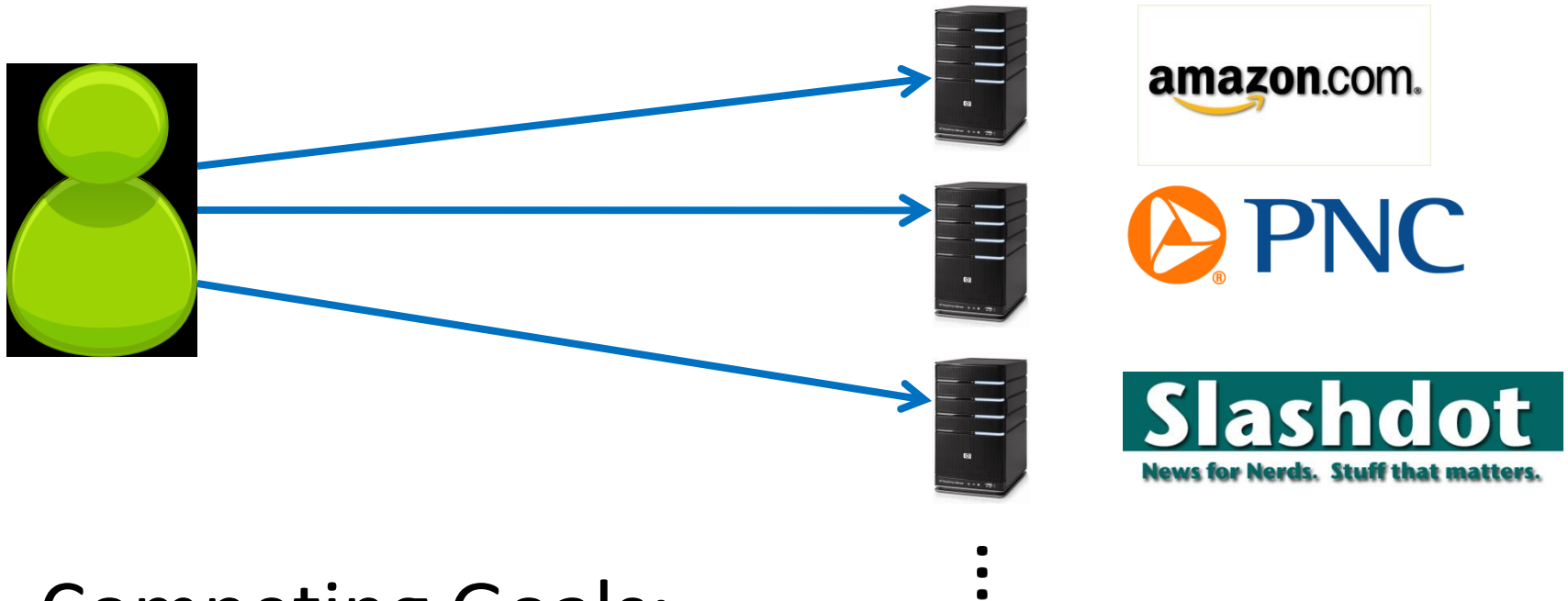


PAO Story #2

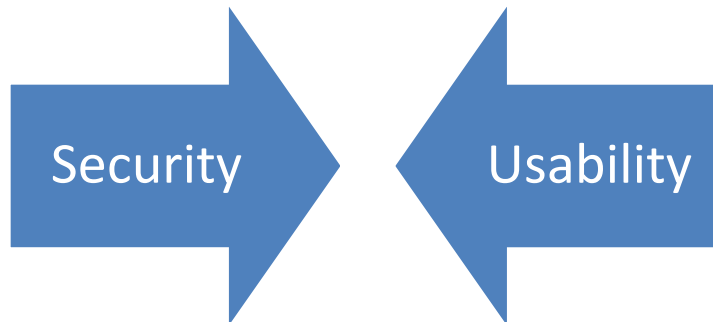


Person	Anupam Datta
Action	Kissing
Object	Piranha

Password Management



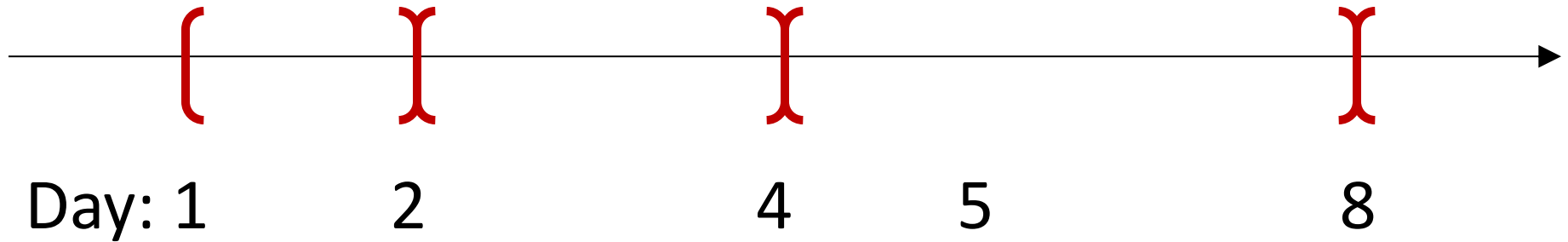
Competing Goals:



Questions

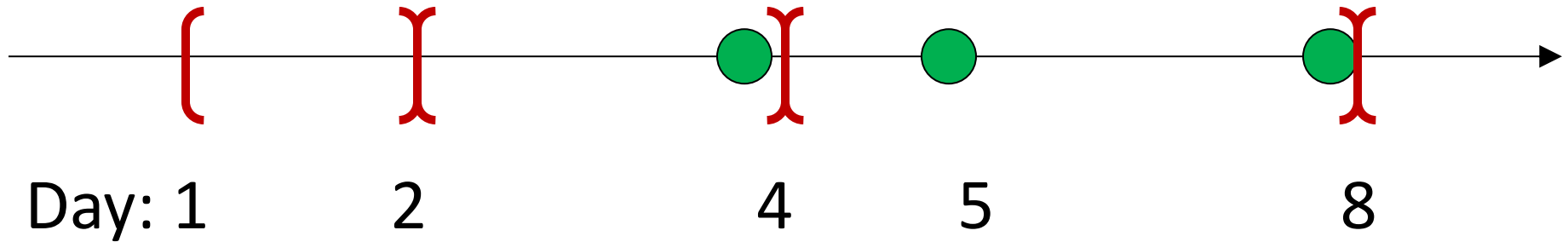
- How can we evaluate password management strategies?
 - Quantify Usability
 - Quantify Security
- Can we design password management schemes which balance security and usability considerations?

Rehearsal Requirement




Expanding Rehearsal Assumption: user maintains cue-association pair by rehearsing during each interval $[s^i, s^{i+1}]$.

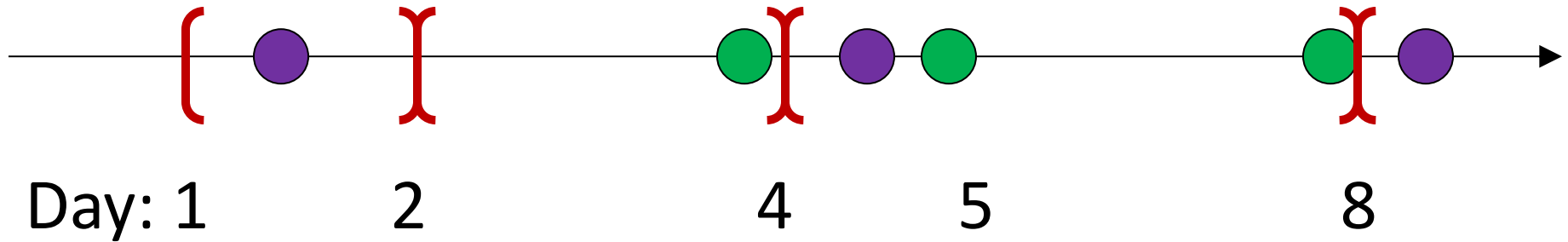
Rehearsal Requirement



Expanding Rehearsal Assumption: user maintains cue-association pair by rehearsing during each interval $[s^i, s^{i+1}]$.

 Visit Amazon: Natural Rehearsal

Rehearsal Requirement



Expanding Rehearsal Assumption: user maintains cue-association pair by rehearsing during each interval $[s^i, s^{i+1}]$.

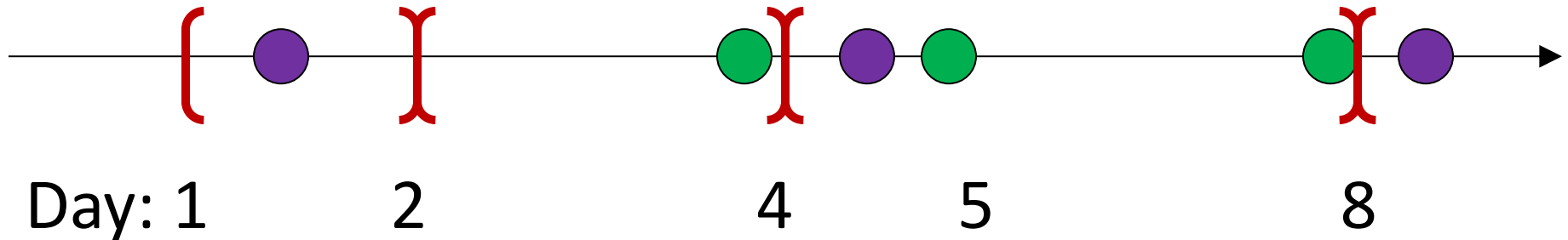


Visit Amazon: Natural Rehearsal



Google

Rehearsal Requirement



Expanding Rehearsal Assumption: user maintains cue-association pair by rehearsing during each interval $[s^i, s^{i+1}]$.



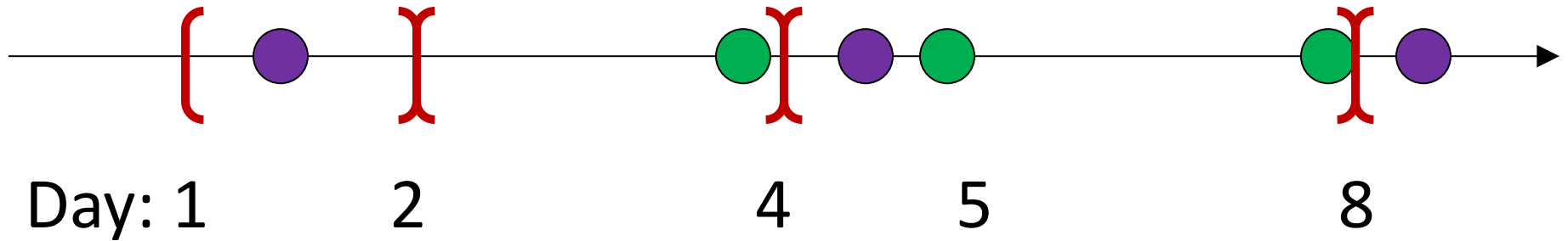
Visit Amazon: Natural Rehearsal



Google

X_t : extra rehearsals to maintain *all* passwords for t days.

Rehearsal Requirement



X_t : extra rehearsals to maintain *all* passwords for t days.

	Reuse Password	Independent Passwords
X_8	0	2

Usability Results

User	Reuse Password	Independent Password
Active	≈ 0	420
Typical	≈ 0	456.6
Occasional	≈ 0	502.7
Infrequent	1.2	564

$E[X_{365}]$: Extra Rehearsals to maintain *all* passwords over the first year.



Usable

Unusable

Our Approach

Public Cue

Private



Action: kicking



Object: penguin

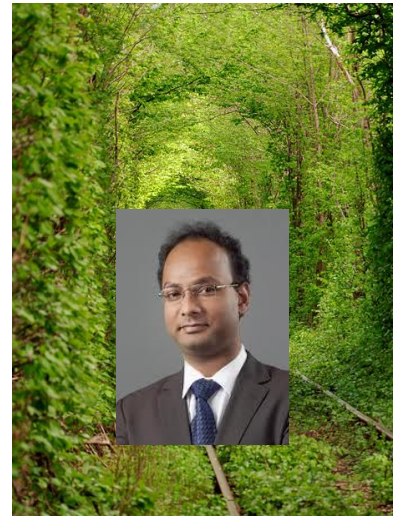


Login

PayPal



...



Pwd

Kic+Pen + Tor + Lio + ... + Kis + Pir

Login

amazon.com.



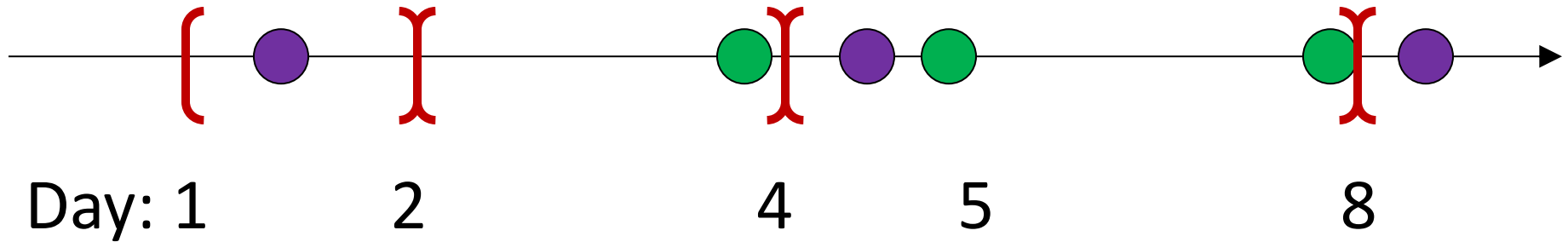
...



Pwd

Kic+Pen +

Sharing Cues



- Usability Advantages
 - Fewer stories to remember!
 - More Natural Rehearsals!
- Security?

(n, l, γ) -Sharing Set Family

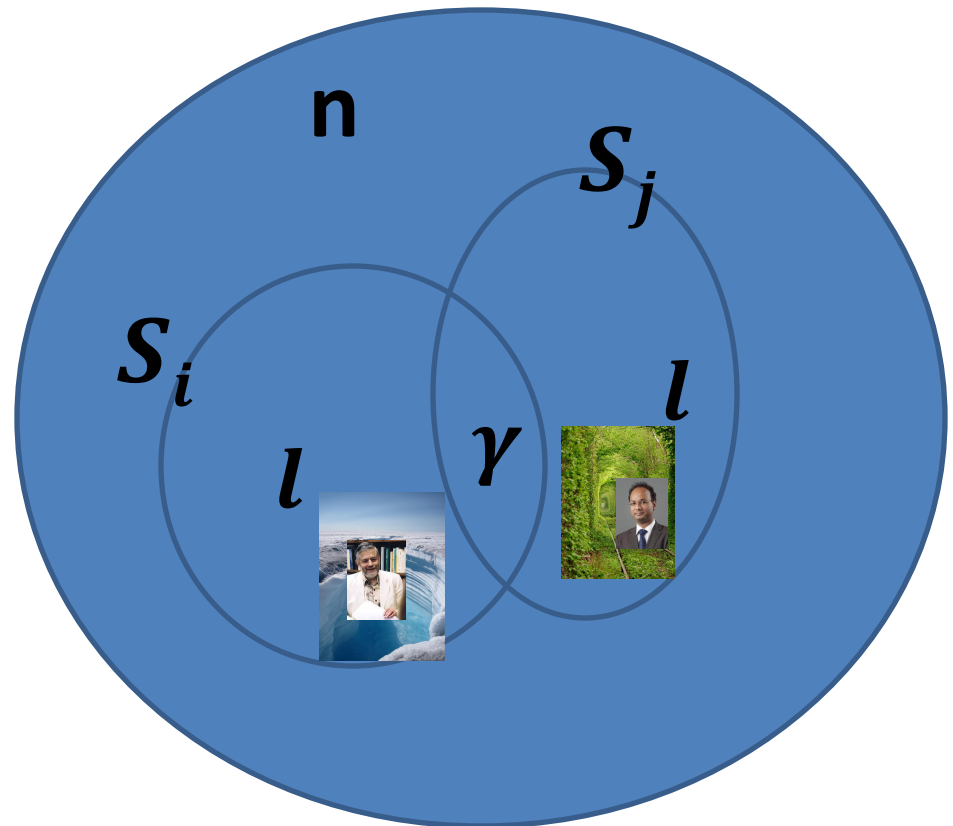
m – number of passwords $\{S_1, \dots, S_m\}$.

n – total #PAO stories

l – #PAO stories for
each site

γ – max intersection

S_i – PAO stories for
account i .



Sharing Cues

Thm: There is a $(43,4,1)$ -Sharing Set Family of size 90, and a $(9,4,3)$ -Sharing Set Family of size 126

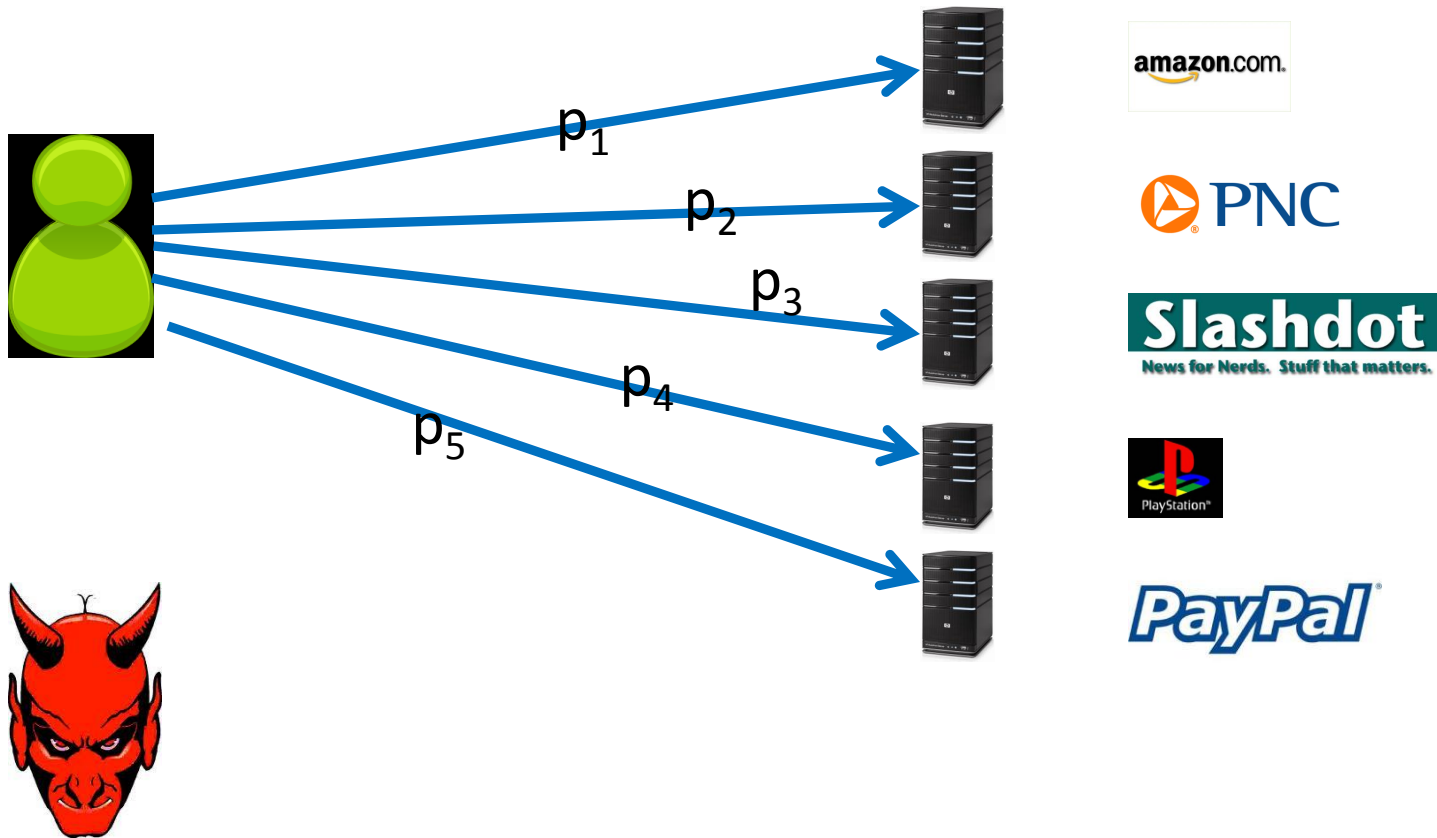
- Proof?
 - Chinese Remainder Theorem!
 - Notice that $43 = 9 + 10 + 11 + 13$ where 9, 10, 11, 13 are pair wise coprime.
 - A_i uses cues: $\{i \bmod 9, i \bmod 10, i \bmod 11, i \bmod 13\}$

Usability Results

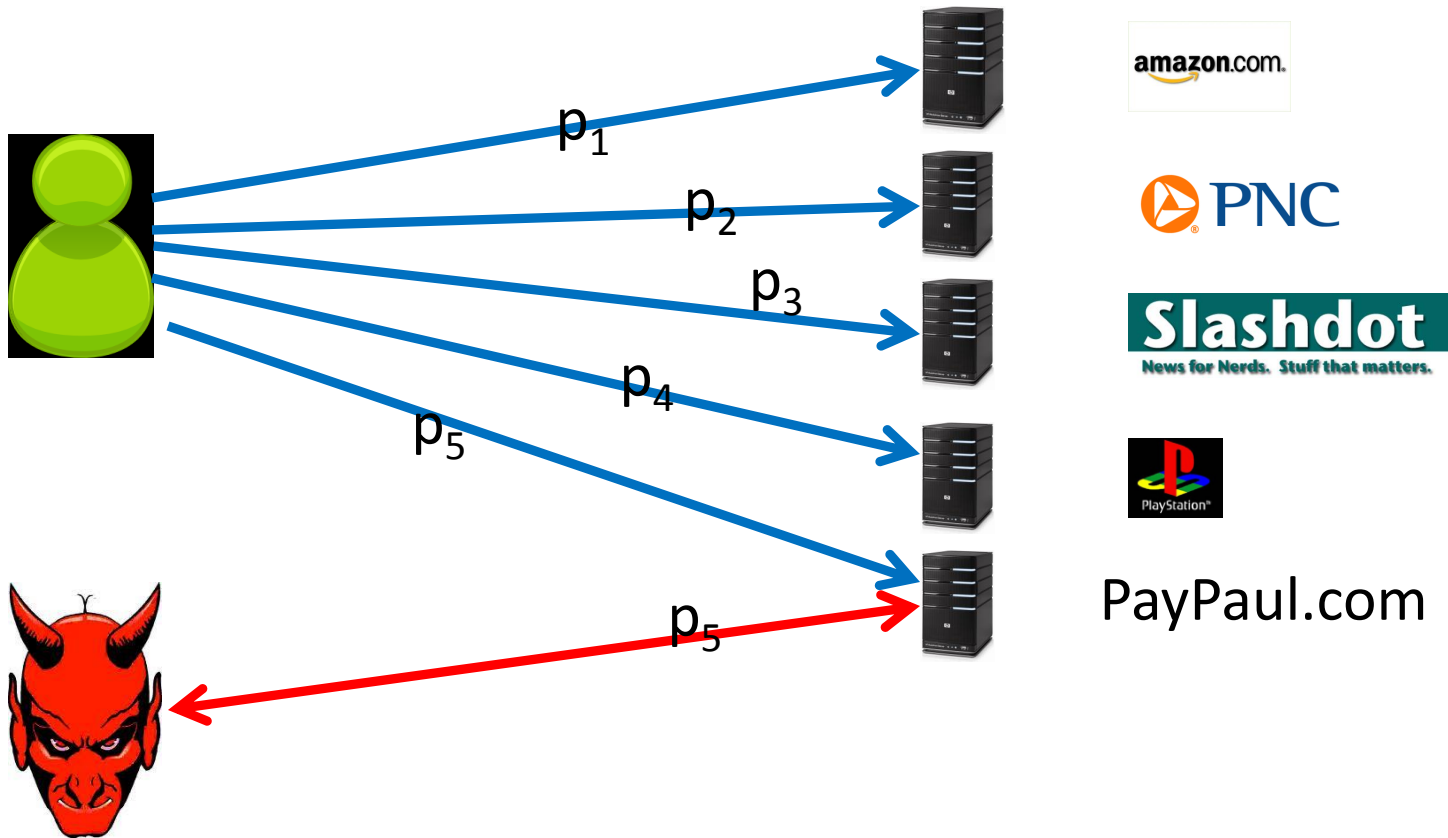
User	Reuse	Independent	(43,4,1)-Sharing	(9,4,3)-Sharing
Active	≈ 0	420	3.93	≈ 0
Typical	≈ 0	456.6	10.89	≈ 0
Occasional	≈ 0	502.7	22.07	≈ 0
Infrequent	1.2	564	119.77	2.44

$E[X_{365}]$: Extra Rehearsals to maintain *all* passwords over the first year.

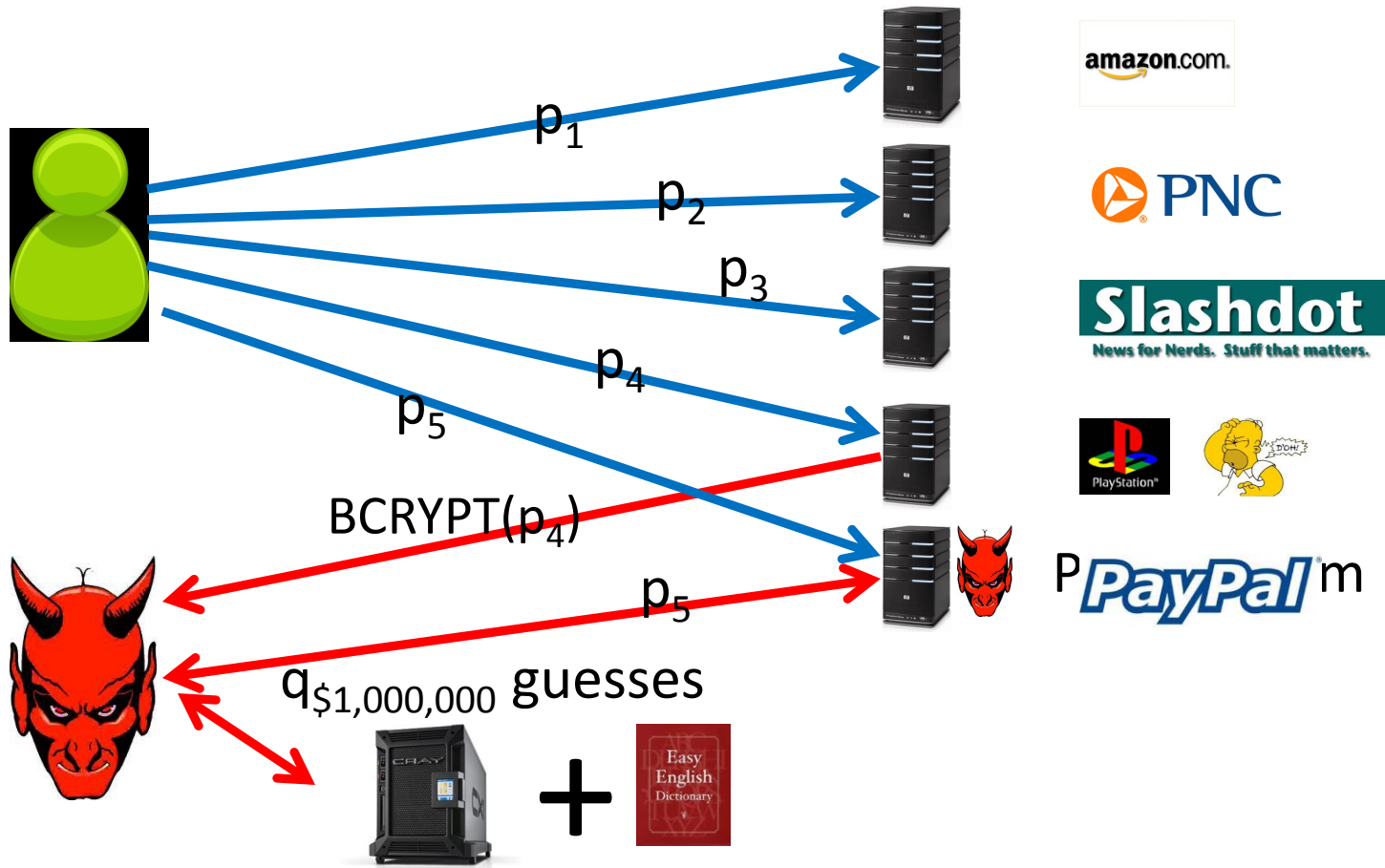
Security as a Game



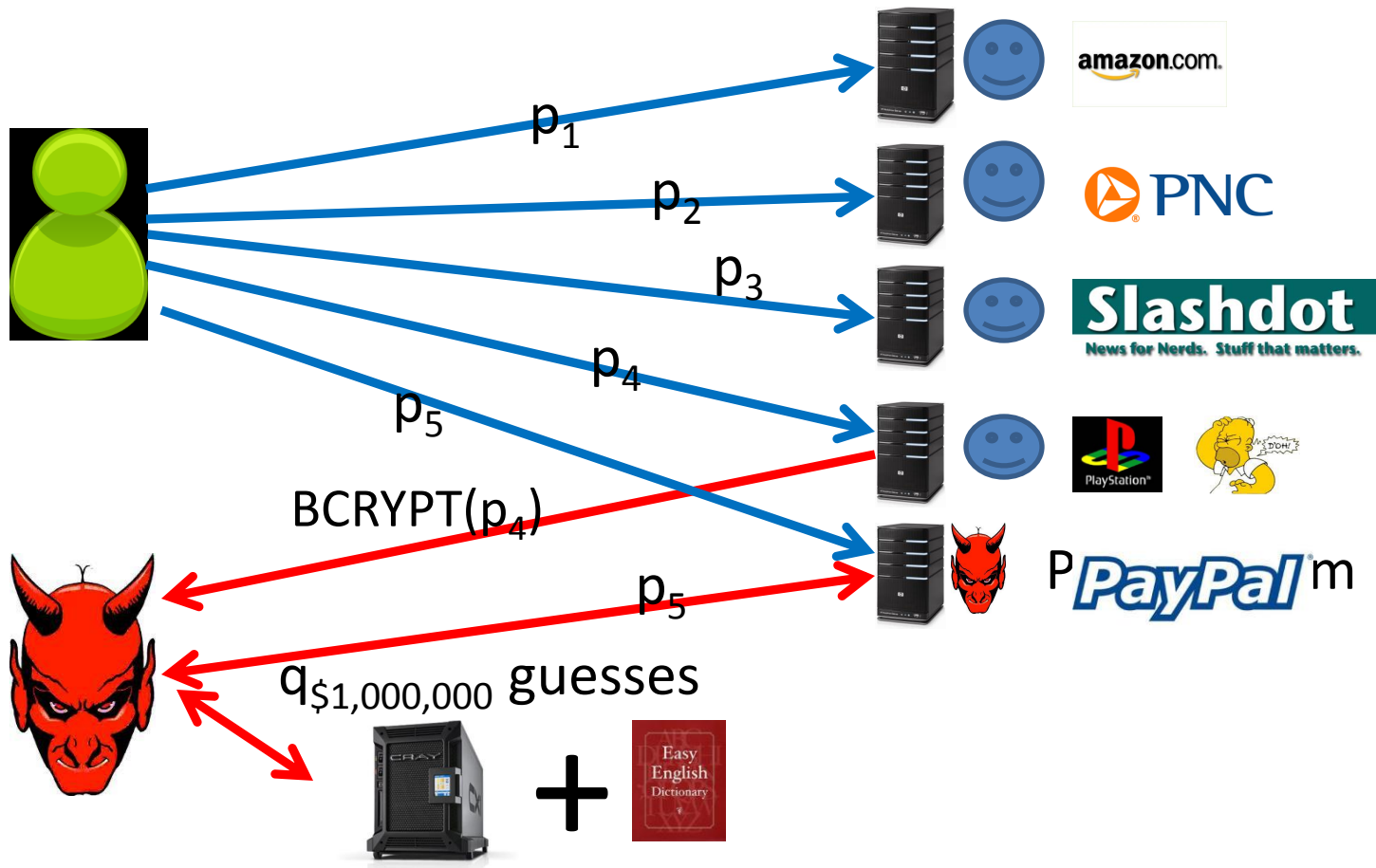
Security as a Game











Security as a Game



Security as a Game



Security Results

Attacks	 r=1	 r=1  h=1	  r=2	  
(n,4,4)-Sharing [Reuse]	No	No	No	No Usable + Insecure
(n,4,0)-Sharing [Independent]	Yes	Yes	Yes	Yes Unusable + Very Secure
(n,4,1)-Sharing	Yes	Yes	Yes	No Usable + Secure
(n,4,3)-Sharing	Yes	No	Yes	No Usable + Pretty Secure

$(q_{\$1,000,000}, \delta, m, 3, r, h)$ -security