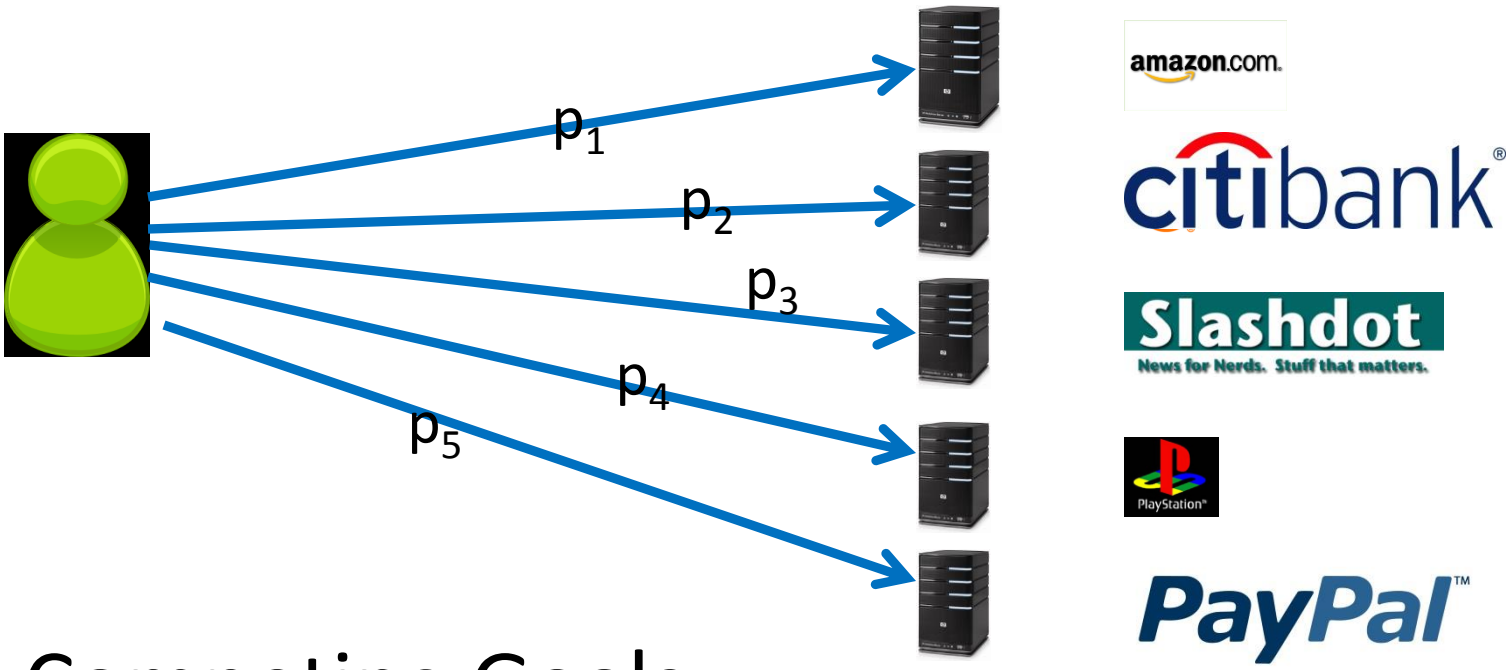
Human-Computable Passwords

Jeremiah Blocki
Manuel Blum
Anupam Datta
Santosh Vempala

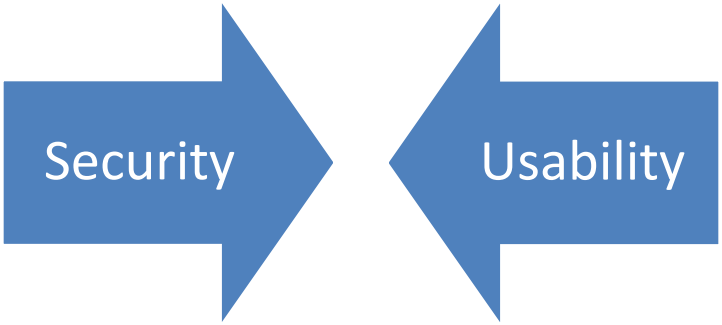
Previous Work

- Naturally Rehearsing Passwords
  - Presentation on Thursday

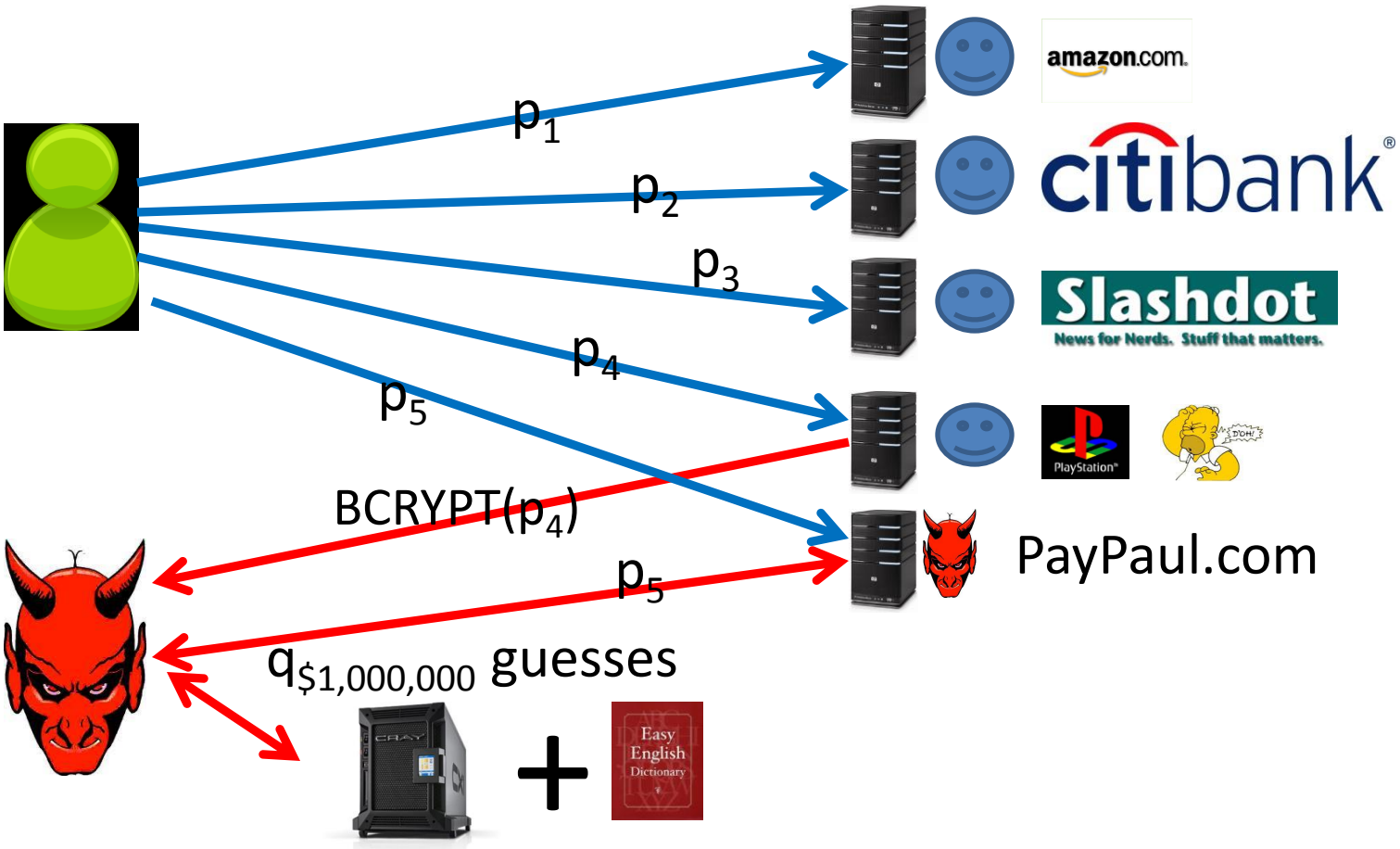
Password Management



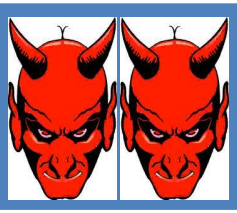
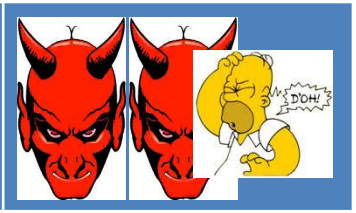
Competing Goals:



Password Security Game



Security Results

Attacks	 k= 1	 k= 1  t=1	 k=2	
Reuse	No	No	No	No
Strong Random Independent	Yes	Yes	Yes	Yes
Shared Cues	Yes	Yes	Yes	No

Usable + Insecure

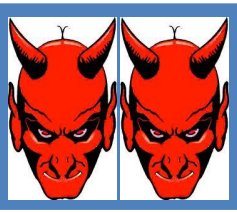
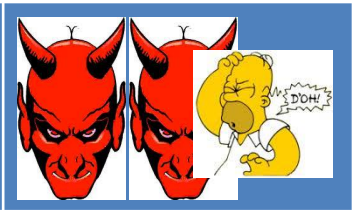
Unusable + Secure

Usable + Secure

 Phishing Attack

 Offline Attack

Security Results

Attacks	 k= 1	 k= 1 t=1	 k=2	
Reuse	**No**	**No**	**No**	**No**
Strong Random Independent	**Yes**	**Yes**	**Yes**	**Yes**
Shared Cues	**Yes**	**Yes**	**Yes**	**No**

Usable + Insecure

Unusable + Secure

Usable + Secure

 Phishing Attack

 Offline Attack

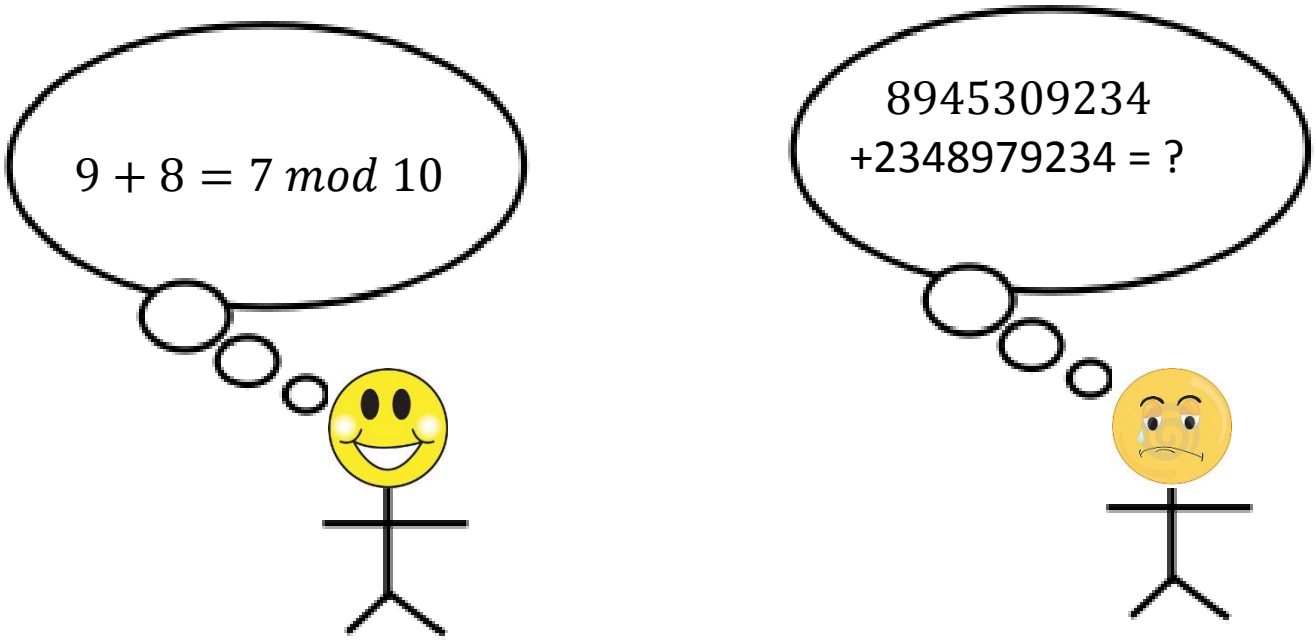
Previous Work

- Naturally Rehearsing Passwords
  - Presentation on Thursday
  - Password Management Scheme: Shared Cues

- Key Question: Can we get better security if we ask the user to perform simple computations to generate his passwords?

Human Computation

- Restricted
  - Simple operations (addition, lookup)
  - Operations performed in memory (limited space)



Human Computation

- Restricted
  - Simple operations (addition, lookup)
  - Operations performed in memory (limited space)
- Improve Security?
  - Simple Computations vs. Pure Recall
  - Security against many breaches?

Candidate Scheme

- Memorize a Random Mapping
  - One time step!
- Password Computed as a Response to Public Challenges
- Required Operations
  - Addition modulo 10
  - Memory lookups

Random Mapping

Image I			…	
σ(I)	9	3	…	6

Initialization:

User Memorizes Random Mapping

$\boldsymbol{\sigma}: \{I_1,\ldots,I_m\} \rightarrow \{0,1,\ldots,9\}$

m images

Single-Digit Challenge




Response:

σ( **) + σ(**  **) = 2 mod 10**

0 
1 
2 
3 
4 
5 
6 
7 
8 
9 

Single-Digit Challenge



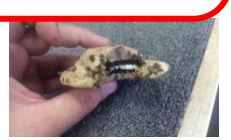

Response:

σ( **) + σ(**  **) = 2 mod 10**

0 
5 

1 
6 

2 
7 

3 
8 

4 
9 

Single-Digit Challenge




Response:

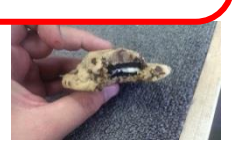
σ  **+ σ**  **+ σ** 

= 7 + 4 + 5 = 6 mod 10

0 
5 

1 
6 

2 
7 

3 
8 

4 
9 

Passwords




Username: jblocki

Password:

σ() + σ() + σ()

= 7 + 4 + 5 = 6 mod 10

0 

1 

2 

3 

4 

5 

6 

7 

8 

9 

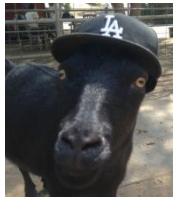
Passwords





Username: jblocki

Password: *

0 

1 

2 

3 

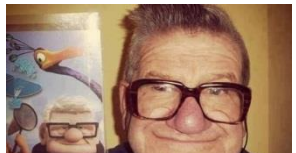
4 

5 

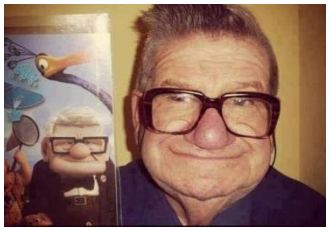
6 

7 

8 

9 

Passwords




Username: jblocki

Password: **

0 
1 
2 
3 
4 

5 
6 
7 
8 
9 

Usability

- Memorization is a one time cost
  - Mapping f is rehearsed naturally
  - Can Add new Images over Time
- Time
  - 75 seconds for a 10 digit password
  - 7.5 seconds per digit (average)

Open Challenge

- Random mapping $\sigma: \{I_1,\ldots,I_{100}\} \rightarrow \{0,1,\ldots,9\}$
- Examples
  - 1000 single-digit challenge response pairs
- Can you crack the code and guess one of the challenge passwords?

http://www.cs.cmu.edu/~jblocki/HumanComputablePasswordsChallenge/challenge.htm

Open Challenge

Function	Secret Length (n)	Challenge Response Pairs	Links	Winner
$f(y_0, \ldots, y_{13}) = y_{13} + y_{12} + y_i \mod 10$ Where $i = y_{11} + y_{12} \mod 10$	100 digits (Pre-solved Example)	500 (e.g., 50 ten digit passwords)	Examples Password Challenges Notebook with Solution	Harry Q. Bovik
	100 digits	1000	Examples Password Challenges	
		500	Examples Password Challenges	
		300	Examples Password Challenges	
	50 digits	500	Examples Password Challenges	
		300	Examples Password Challenges	
		150	Examples Password Challenges	
	30 digits	300	Examples Password Challenges	
		100	Examples Password Challenges	
		50	Examples Password Challenges	
$f(y_0, \ldots, y_{13}) = y_{11} + y_{12} + y_{13} + y_i \mod 10$ Where $i = y_{10} \mod 10$	100 digits (Pre-solved Example)	500 (e.g., 50 ten digit passwords)	Examples Password Challenges Notebook with Solution	Harry Q. Bovik
	100 digits	500	Examples Password Challenges	
		300	Examples Password Challenges	
		200	Examples P	
	50 digits	300	Examples P	
		150	Examples P	
		100	Examples P	
	30 digits	150	Examples P	
		100	Examples P	
		50	Examples P	

http://www.cs.cmu.edu/~jblocki/HumanComputablePasswordsChallenge/challenge.htm