Secondary and partial passwords: Are they secure and usable?

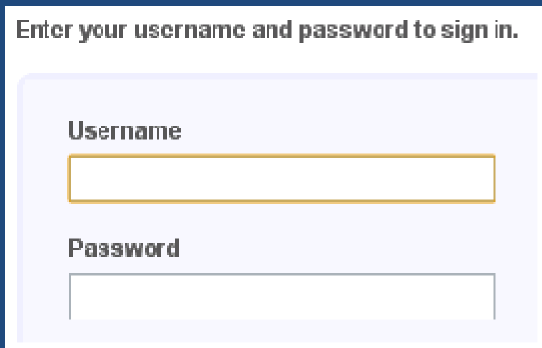
Mike Just, Heriot-Watt University

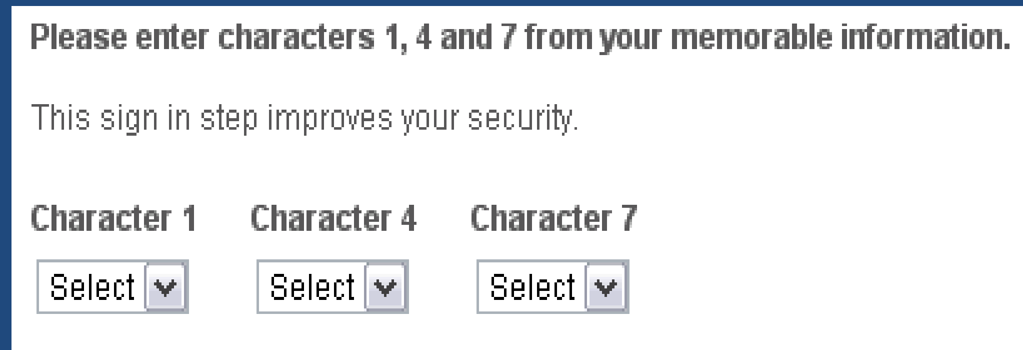
COINS Summer School on Auth Ecosystems

31 July 2016

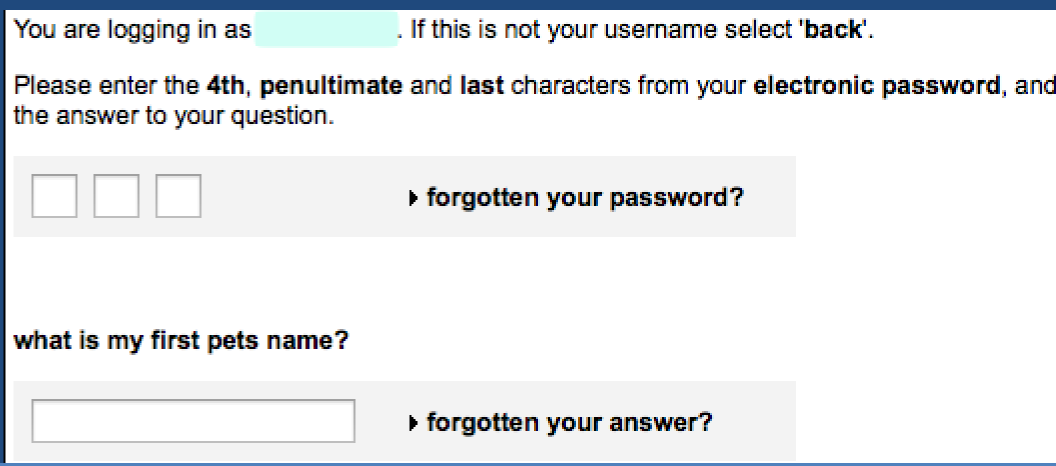
Some recent observations (1)

Login screens at Halifax Bank of Scotland





Login screens at First Direct



Some recent observations (2)

Bank	Cred. B1	Credential B2
1) FD	Challenge quest.	Partial password
2) Smile	Partial PIN	Challenge quest.
3) HBoS	Password	Partial password
4) NatWest	Partial PIN	Partial password
5) Santander	Password	PIN
6) Barclays	PIN	Partial password
7) Citibank	Password	Challenge quest.
8) B. of Ireland	PIN	Partial PIN
9) HSBC	Challenge quest.	PIN
10) AIB	Partial PIN	Challenge quest.

- Different types of credentials
- Different combinations (no two are the same)
- Varying parameters: alphabet, length, “partial” query, questions, question #s

Some recent observations (3)

- Apparent concerns about security of single credentials (passwords, PINs, challenge questions, “partial” variations)
- Different attacks: guessing, recording
- Wide variety of implementation choices
  - Other differences: attempts allowed, update requirements, …
  - Suggests confusion?
  - Variety is good (e.g., limiting credential re-use)?
- What can we say about security/usability?

Outline

- Part I: Properties of dual credential authentication
  - Security and usability
  - [ICITST 2012]
- Part II: Security of partial password/PIN authentication
  - [Financial Cryptography 2013]
- Concluding remarks

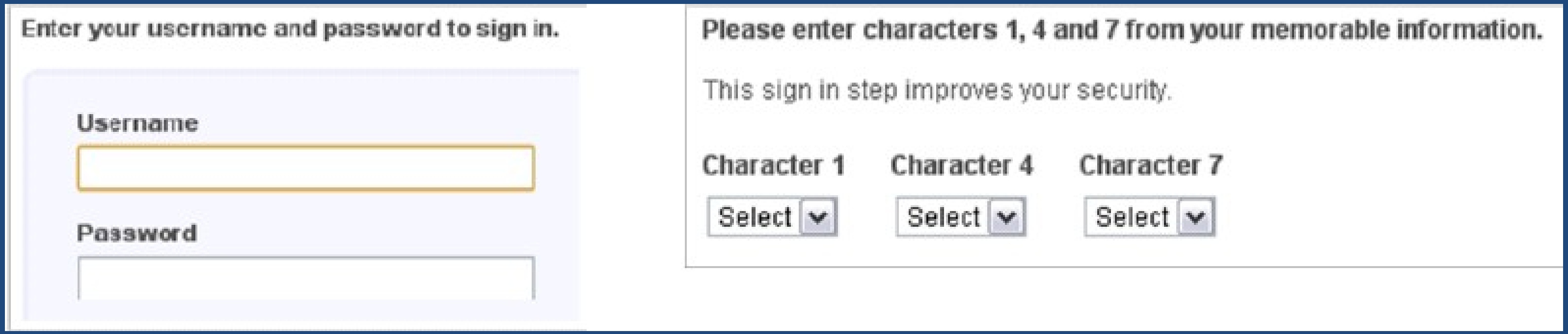
Part I:
Properties of dual credential authentication

Motivation: Single Credential Errors

- Failure from poor implementation decision
- Example: userID and single password
    - Errors with either should result in **atomic** response
- Bonneau and Preibusch (2010) found that 19% of 150 websites provide a granular response
    - This allows an attacker to guess valid userIDs
    - Easy to mitigate

Issue: Dual Credential Errors

- Same issue, though additional complexity
- Suppose user enters userID and two credentials

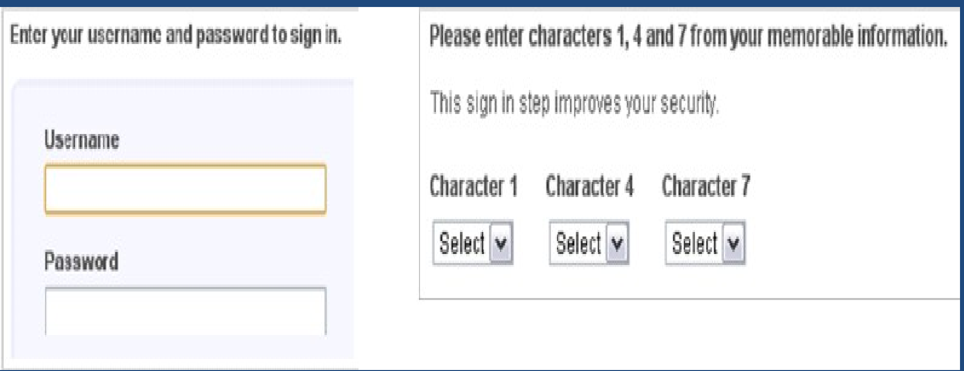


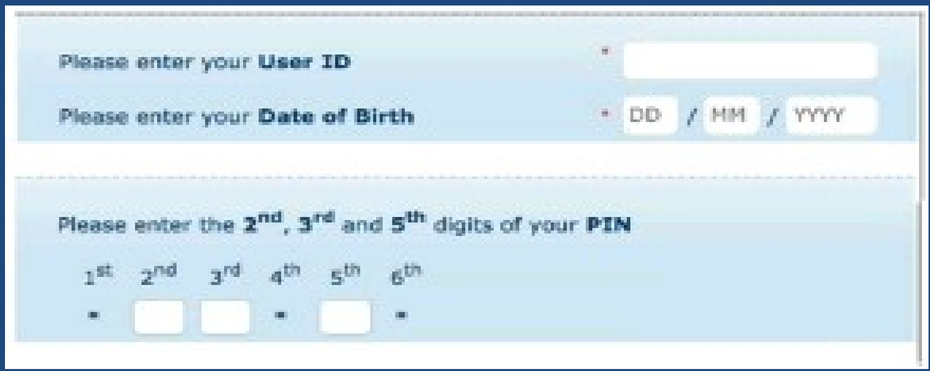
- Should atomicity cover all three components?
- Or just the credentials? Or userID & first credential?

Authentication Interaction Patterns

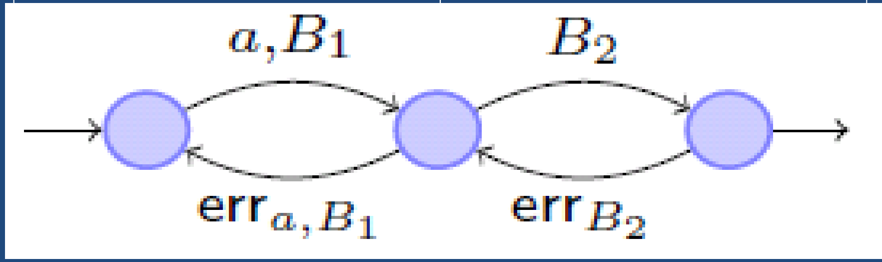
- Patterns in processing of credentials
  - userID (a) and two credentials (B1 and B2)
1. Screen or Submission Point (SP) (“|”)
   - Submission of components, observed as new screen
   - E.g., *aB1|B2, a|B1B2, …*
2. Feedback or Validation Point (FP) (“+”)
   - *When* feedback is provided to user
   - E.g., *aB1B2+*
3. Feedback Atomicity (FA) (“()”)
   - *What* feedback is provided to user
   - E.g., *(aB1)(B2)*

Interaction Patterns – Two Examples

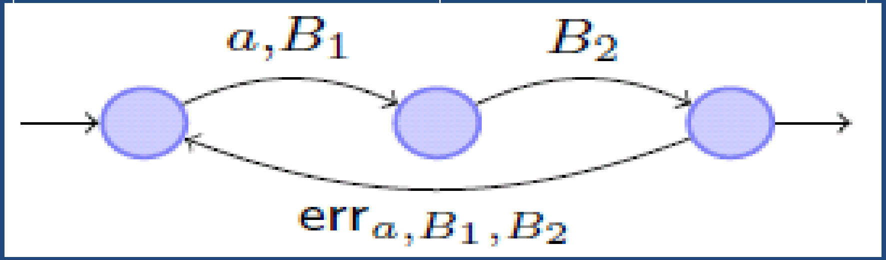




Screen Point	aB1|B2|
Feedback Point	aB1+B2+
Feedback Atomicity	(aB1)(B2)



Screen Point	aB1|B2|
Feedback Point	aB1B2+
Feedback Atomicity	(aB1B2)



Authentication Pattern Summary

- Four pattern possibilities for each pattern type
- Three pattern types composable in $4^3=64$ ways
  - Though only 25 of the compositions are valid (see paper)

Pattern #	Pattern Type: Screen Point	Pattern Type: Feedback Point	Pattern Type: Feedback Atomicity
I	$aB_1\|B_2\|$	aB_1+B_2+	$(aB_1)(B_2)$
II	$a\|B_1B_2\|$	$a+B_1B_2+$	$(a)(B_1B_2)$
III	$a\|B_1\|B_2\|$	$a+B_1+B_2+$	$(a)(B_1)(B_2)$
IV	$aB_1B_2\|$	aB_1B_2+	(aB_1B_2)

Authentication Patterns of UK Banks

Bank Name	Screen Point	Feedback Point	Feedback Atomicity	Pattern Desc.	Pattern Composition
FI-3 FI-7	$aB_1\|B_2\|$	aB_1+B_2+	$(aB_1)(B_2)$	I-I-I	$(aB_1)+(B_2)+$
FI-8	$aB_1\|B_2\|$	aB_1B_2+	(aB_1B_2)	I-IV-IV	$(aB_1\|B_2)+$
FI-1 FI-4 FI-9 FI-6	$a\|B_1B_2\|$	$a+B_1B_2+$	$(a)(B_1B_2)$	II-II-II	$(a)+(B_1B_2)+$
FI-5 FI-10	$a\|B_1B_2\|$	aB_1B_2+	(aB_1B_2)	II-IV-IV	$(a\|B_1B_2)+$
FI-2	$a\|B_1\|B_2\|$	aB_1B_2+	$(a)(B_1B_2)$	III-IV-II	$(a)\|(B_1\|B_2)+$

Authentication Patterns and Usability (1)

U1. Granular credential feedback
- If error in *B1* or *B2*, user is informed which is incorrect
- Described by FA ("()")
- E.g., *(aB1)+(B2)* is granular, *(aB1|B2)+* is atomic

U2. Timely credential feedback
- If providing feedback, do it at point of submission
- Described by relationship between FP ("+") and FA ("()")
- E.g., *(a)|(B1|B2)+* provides granular info about "*a*", but not till end

U3. Immediate feedback provision
- If introducing a new screen, then provide feedback on new screen
- Described by relationship between SP ("|") and FP ("+")
- E.g., *(a|B1B2)+* provides a screen after "*a*", but no feedback till end

Authentication Patterns and Usability (2)

Bank Name	Pattern Desc.	Pattern Composition	Usability Properties			
			# Screens	U1	U2	U3
FI-3 FI-7	I-I-I	$(aB_1)+(B_2)+$	2	Y	Y	Y
FI-8	I-IV-IV	$(aB_1\|B_2)+$	2	No	Y	No
FI-1 FI-4 FI-9 FI-6	II-II-II	$(a)+(B_1B_2)+$	2	No	Y	Y
FI-5 FI-10	II-IV-IV	$(a\|B_1B_2)+$	2	No	Y	No
FI-2	III-IV-II	$(a)\|(B_1\|B_2)+$	3	No	No	No

Heriot-Watt University

interactive & trustworthy technologies

Authentication Patterns and Security (1)

- Based upon FA ("()") and credential parameters
- Atomicity of userID (a) and first credential (B1)
  - Same as case investigated by Bonneau and Preibusch
- Atomicity of credentials B1 and B2
  - Tradeoff with U1: Either atomic or granular feedback
  - If atomic: Must attack credentials simultaneously (*x*)
  - If granular: Can attack credentials separately (*+*)
  - Depends upon purpose of second credential

Authentication Patterns and Security (2)

Bank ID	Pattern Desc.	userID protected?	Credential Security	Guesswork Estimate
FI-3 FI-7	I-I-I	Y	add.	$2^{22}+2^{12} \approx 2^{22}$ $2^{22}+2^{12} \approx 2^{22}$
FI-8	I-IV-IV	Y	$\times$	$2^{12} \times 2^{9} \approx 2^{21}$
FI-1 FI-4 FI-9 FI-6	II-II-II	No	$\times$	$2^{12} \times 2^{12} \approx 2^{24}$ $2^{6} \times 2^{12} \approx 2^{18}$ $2^{12} \times 2^{12} \approx 2^{24}$ $2^{12} \times 2^{9} \approx 2^{21}$
FI-5 FI-10	II-IV-IV	Y	$\times$	$2^{22} \times 2^{12} \approx 2^{34}$ $2^{9} \times 2^{12} \approx 2^{21}$
FI-2	III-IV-II	No	$\times$	$2^{6} \times 2^{12} \approx 2^{18}$

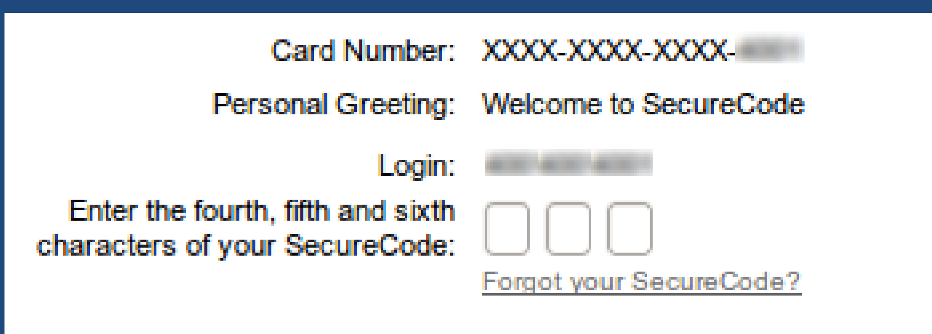
Dual credential authentication properties

- Some apparent impacts on usability
  - Variation in terms of presentation and feedback
  - Potential for confusion for users
  - Still needs to be confirmed experimentally
- Some impacts upon security
  - Guessing of userIDs or not
  - Guessing of credentials independently
  - Parameter choices
- Impact of using account-specific challenges
- Next step: Evaluate usability with real users

Part II:
Security of partial password/PIN

Partial Password Security

- Focus on a specific form of authentication
- Partial password authentication
  - Challenge for 2-3 positions of a password
  - Password characters at the positions are the response
- Motivation: Don't reveal password in one step



Who uses partial passwords?

Bank	N	n	m	Bank	N	n	m
ING DiBa	10	6	2	Nat West 2	36	6-20	3
Coop	10	4	2	HBoS	36	6-15	3
Tesco	10	6	2	3DSecure (B. of Ireland)	36	8-15	3
Smile	10	6	2	Standard Life	36	8-10	3
Nationwide	10	6	3	Skipton	36	8-30	3
AIB	10	5	3	First Direct	36	6-30	3
B. Of Ireland	10	6	3	Barclays	52	6-8	2
Nat West 1	10	4	2	HSBC (Canada)	62	8	3

N: character set size
n: password length
m: challenge size

Attack model

- User enters userID and two credentials (one is a partial password or PIN)
- Attacks (focus on partial password/PIN)
  - *Online guessing*, based on knowledge of alphabet
  - *Recording* previous challenge-response pairs
  - *Recording + Guessing* yields most optimal attacks
- Sample cases *(N,n,m)*
  - PIN: *(10, 6, 2)* with *B=6* guesses
  - Password: *(36, 8, 3)* with *B=10* guesses

Guessing – Brute force

- Strategy: B guesses of next challenge
- B success rate: BN^{-m}

Attack type	PIN case	Password case
Brute force	6 %	0.002 %

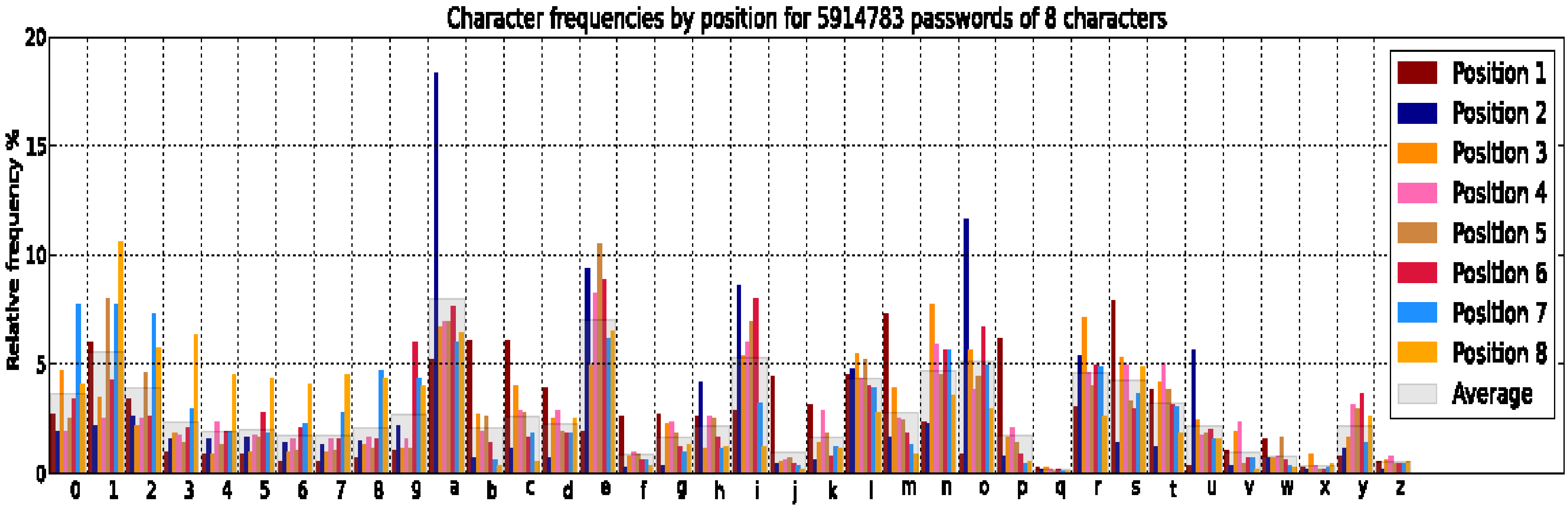
Guessing – Dictionary

- Strategy: Guess the top *B* passwords/PINs in sorted dictionary
  - Same as guessing full (non-partial) password
- RockYou passwords
  - password (1.01%), iloveyou (0.84%), princess (0.56%), …
- RockYou PINs
  - 123456 (12.76%), 654321 (0.61%), 111111 (0.58%), …

Attack type	PIN case	Password case
Brute force	6 %	0.002 %
Dictionary	15.3 %	3.9 %

Guessing – Letter position frequency (1)

- Based upon frequency of letters indifferent positions
  - ‘a’ occurs 8% in RockYou, but 18% in position 2
  - ‘1’ occurs 17% in RockYou, but 40% in position 1



HERIOT WATT UNIVERSITY

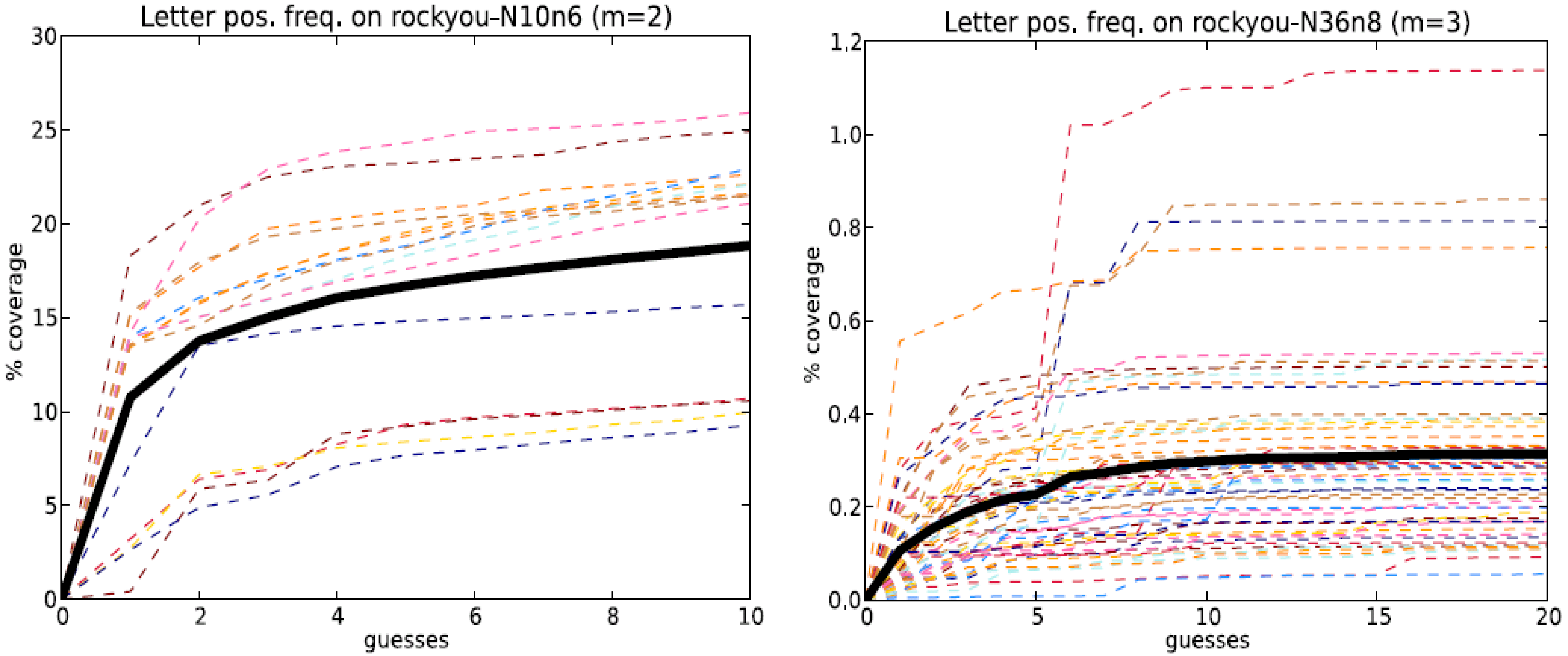
interactive & trustworthy technologies

Guessing – Letter position frequency (2)

- Strategy: Guess ith most frequent character in each position at guess i
- Strategy not optimal since dependencies are not considered

Attack type	PIN case	Password case
Brute force	6 %	0.002 %
Dictionary	15.3 %	3.9 %
Letter position	17.2 %	0.3 %

Guessing – Letter position frequency (3)

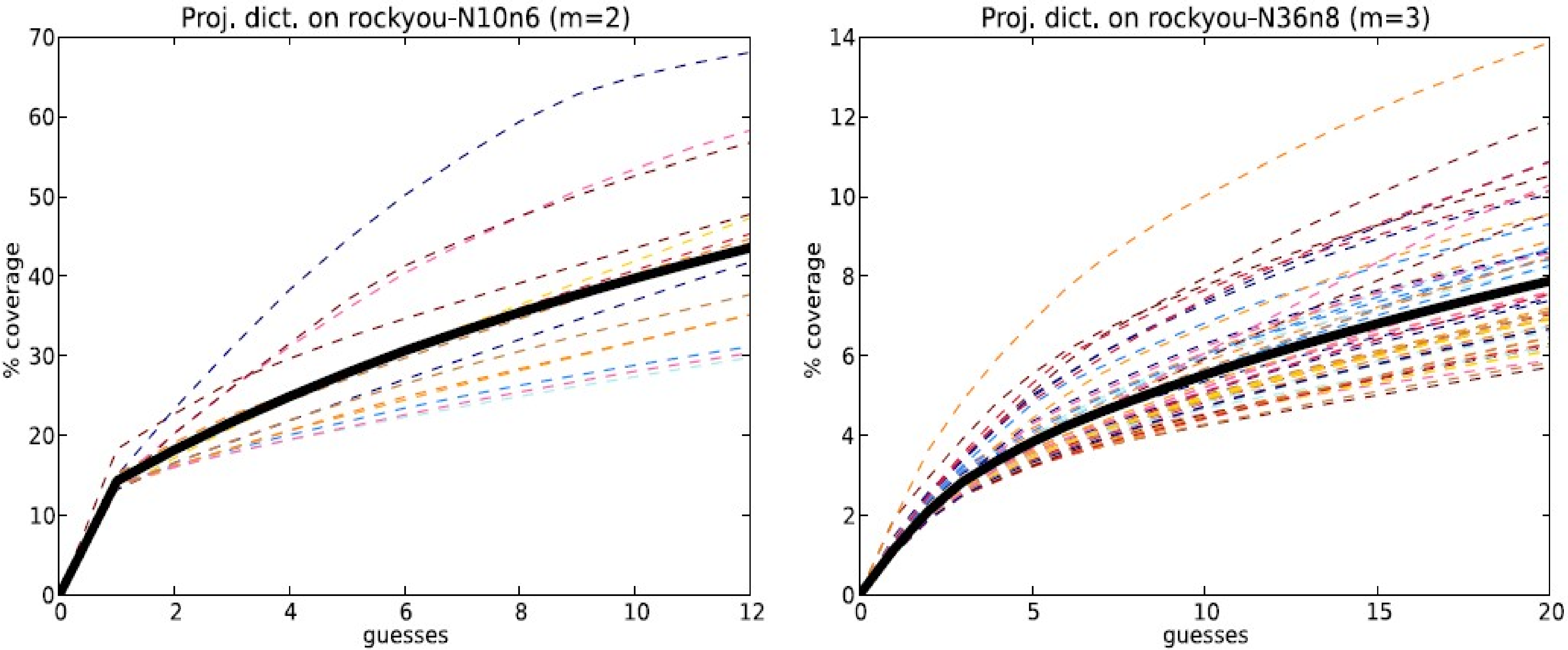


Guessing – Projection dictionary (1)

- Observation: Many words share same projection onto a set of challenge positions
- Top RockYou passwords: password (1.01%), iloveyou (0.84%)
- Top {1,2,3} challenge responses: {i,l,o} (1.29%), {p,a,s} (1.13%)
- Strategy: Guess the top B projections for each challenge

Attack type	PIN case	Password case
Brute force	6 %	0.002 %
Dictionary	15.3 %	3.9 %
Letter position	17.2 %	0.3 %
Projection dictionary	30.6 % (22 % to 50 %)	5.5 % (4.2 % to 10 %)

Guessing – Projection dictionary (2)



Recording attacks (1)

- Claimed benefit of partial passwords is to mitigate recording (observation attacks)
- So how effective are recording attacks?
- PIN case $(n=6, m=2)$: $C(n,m) = 15$
- Password case $(n=36, m=3)$: $C(n,m) = 56$
- After recording > 1 challenge-response
  - $\{1,3,5\}$ and $\{2,4,5\}$ allow guessing of $\{1,2,4\}$, …

Recording attacks (2)

- How quickly are positions learned?
- Probability of recording *i* positions after *k* runs

$$p_n^m(i,k) = \begin{cases} \frac{1}{\binom{n}{m}} \sum_{j=0}^{m} \binom{i-j}{m-j}\binom{n-(i-j)}{j} p_n^m(i-j,k-1) & m \le i \le n,\ k \ge 1 \\ 1 & i=0,\ k=0 \\ 0 & \text{otherwise} \end{cases}$$

- Recursive, based upon probability after run *k-1*
- Mix of new positions (*j*) and ones already seen (*m-j*)

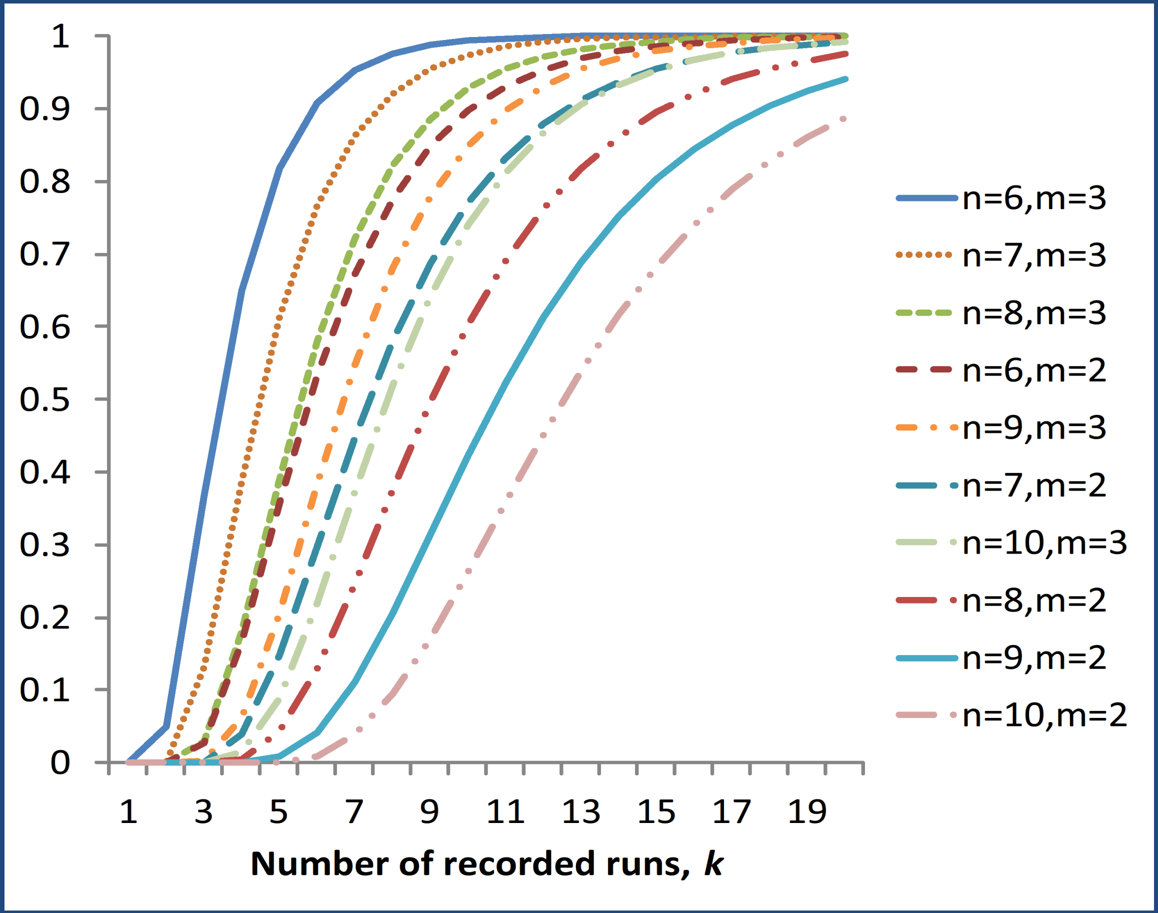
Recording attacks (3)

- Example: *m=2*, probability of *i=4* positions after *k=3* runs

$$p_n^2(4,3) = \frac{1}{\binom{n}{2}} \left[\binom{4}{2} p_n^2(4,2) + \binom{3}{1}\binom{n-3}{1} p_n^2(3,2) + \binom{n-2}{2} p_n^2(2,2) \right]$$

- *C(4,2)* ways to choose *2* positions from *4* already learned
- *C(3,1)* ways to choose an already observed position, and *C(n-3,1)* to choose a new position
- *C(n-2,2)* ways to choose two new positions
- For example, $p^2_{10}(4,3) \approx 0.26$

Recording attacks – Learning full password



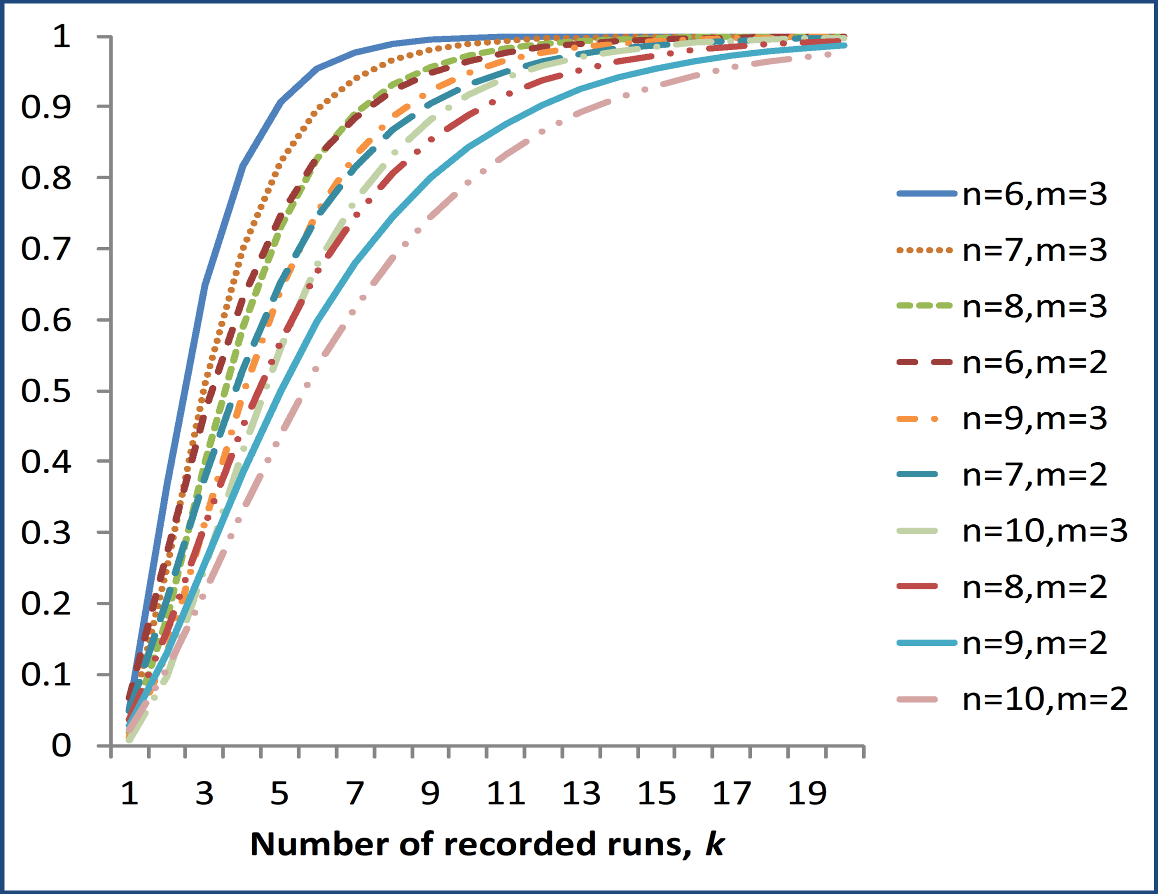
- Both password and PIN cases take *k=6* runs before *> 50%* probability

Recording attacks – Learning next challenge (1)

- Given $i \leq n$ known positions, how many challenges are known?
- Proportion of challenges known after k runs

$$s_n^m(i) = \frac{\binom{i}{m}}{\binom{n}{m}} \qquad \overline{s_n^m}(k) = \sum_{i=m}^{n} p_n^m(i,k)\, s_n^m(i)$$

Recording attacks – Learning next challenge (2)



- Both password and PIN cases take *k=4* runs before > *50%* probability

Recording and guessing (1)

- Given *i* known positions, how many challenges are known that have $m' \leq m$ known positions?
- Can compute proportion of challenges known after *k* runs that have $m' \leq m$ known positions

$$s_n^m(i, m') = \frac{\binom{i}{m'}\binom{n-i}{m-m'}}{\binom{n}{m}} \qquad \overline{s_n^m}(k, m') = \sum_{i=m}^{n} p_n^m(i, k)\, s_n^m(i, m')$$

Recording and guessing (2)

- Can compute the overall success rate given the rate when different numbers of positions are known

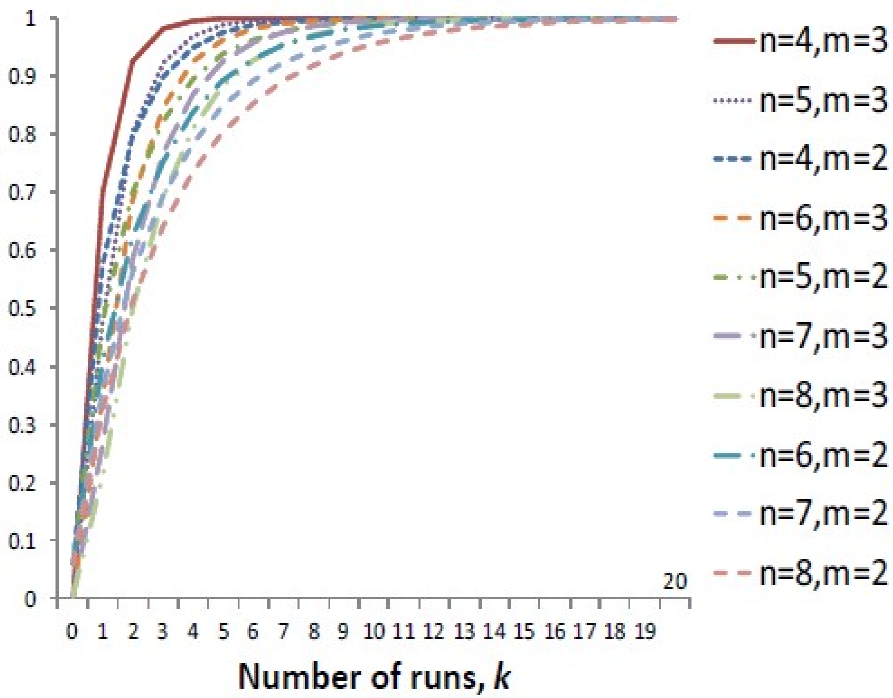
$$\sum_{j=0}^{m} \overline{s_n^m(k,j)} w_j$$

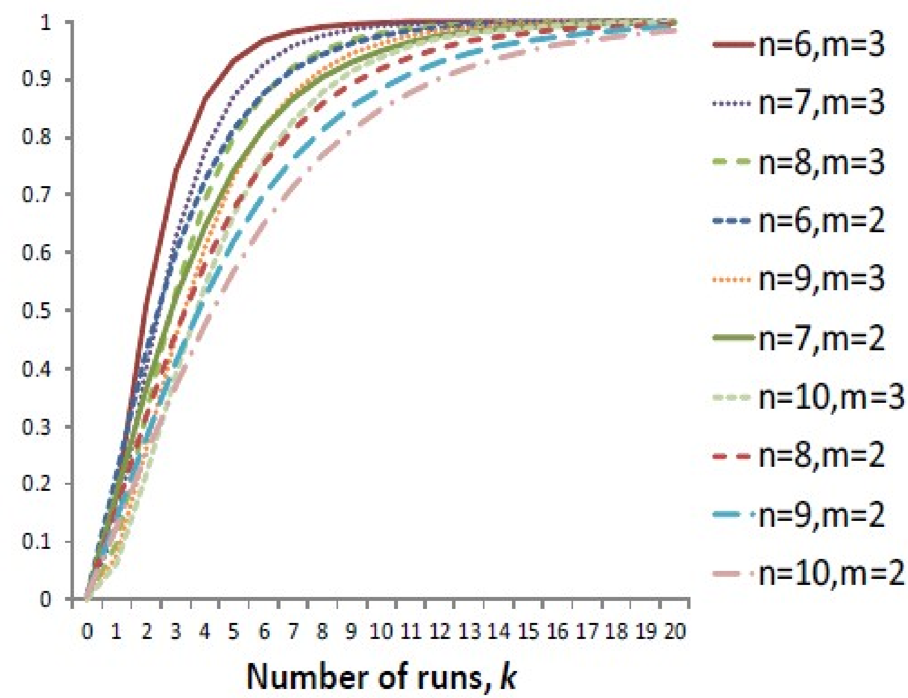
- Depends on N (alphabet size) & B (# of guesses)
- For brute force, at most $N^{m\text{-}m'}$ guesses

$$w_j = \begin{cases} 1 & \text{if } N^{m-j} \leq \beta \\ \frac{\beta}{N^{m-j}} & \text{otherwise} \end{cases}$$

Recording and guessing (3)

- PIN case (left): *k=2* before > *50%* probability
- Password case (right): *k=3* before > *50%* probability





HERIOT WATT UNIVERSITY

interactive & trustworthy technologies

Recording and guessing – Beyond BF (1)

- We can do better than brute force (BF) guessing
- Use the best of letter position, and projection dictionary
- Password case
  - $w_0 = 5.5\ \%$ (projection dictionary)
  - $w_1 = 12\ \%$ (projection dictionary for $m=2$ case)
  - $w_2 = 60\ \%$ (letter position frequency)
  - $w_3 = 100\ \%$ (all positions known)
- Password case: $k=2$ before $> 50\%$ probability
- PIN case: $k=1$ before $> 50\%$ probability

Recording and guessing – Beyond BF (2)

Attack type	PIN case	Password case
Brute force	6 %	0.002 %
Dictionary	15.3 %	3.9 %
Letter position	17.2 %	0.3 %
Projection dictionary	30.6 %	5.5 %
Recording, k=1 (k=4)	6.7 % (63.1 %)	1.8 % (59.0 %)
Recording + BF, k=1 (k=4)	41.1 % (83.8 %)	9.6 % (69.1 %)
Recording ++, k=1 (k=4)	60.2 % (90.4 %)	25.2 % (81.2 %)

- These are lower bounds

Concluding Remarks (1)

- Identification of security and usability differences with dual credential authentication implementations
- Introduced patterns for comparing approaches
  - Potential to expand this further
- Initial work suggests some room for improvement in terms of security and usability
  - Though further study required

Concluding Remarks (2)

- Partial passwords
  - Limited security protection, especially the low number of observations required
  - Caveat: RockYou database is an approximation
  - Further work: response recovery only, different challenge formats, refine the guessing probabilities