

# PASSWORD STRENGTH ANALYSIS

## COPING MECHANISMS IN PASSWORD SELECTION

Brian Curnett and Teri Flory

Masters Students



The Center for Education and Research  
in Information Assurance and Security

# CURRENT STATUS

## Problem Statement

Stringent requirements in password policies lead to coping mechanisms in users when creating passwords. These coping mechanisms decrease the strength of the passwords created, and the question is whether this decreases the security sought by creating a strict policy.

## Work accomplished

- Literature Review
- Methodology
- Consent forms
- Data Management Plan
- Fake passwords
- Entropy (data) calculated on fake passwords
- Statistical consulting
- Proposal
- IRB
  - Submitted and Resubmitted
- Surveys
- Coping Mechanisms
- Post Coping Mechanism Entropy
- Mechanical Turk HIT and link
- Website Development

# COPING MECHANISMS IDENTIFIED

## ANALYSIS OF COPING MECHANISMS IN USER CREATED PASSWORDS

	Coping Mechanism Identified	Decrease in Entropy
A	Repeating digits within the same password	Divide actual entropy by the number of repeats
B	Repeating passwords across time	Subtract entropy for the portion repeated
C	Incrementing numbers across time	Decrease entropy by 6 (entropy gained by adding non-alphanumeric characters)
D	Repeating non-alphabetic or capital letters	Decrease entropy by 6 (entropy gained by adding non-alphanumeric characters)
E	Changing letter from lowercase to capital, but keep the same word across time	Subtract entropy for the word, but maintain the increase of 6 for the capital letter
F	Capital letter first or number/special character last	Decrease entropy by 6 (entropy gained by adding non-alphanumeric character or capital letter)

# POLICIES

## COMPREHENSIVE 8

- At Least 8 characters
- At least one lower case character
- At least one capital letter
- At least one number
- At least one special character

## BLACKLIST HARD

- At least 8 characters
- No English words

## BASIC 16

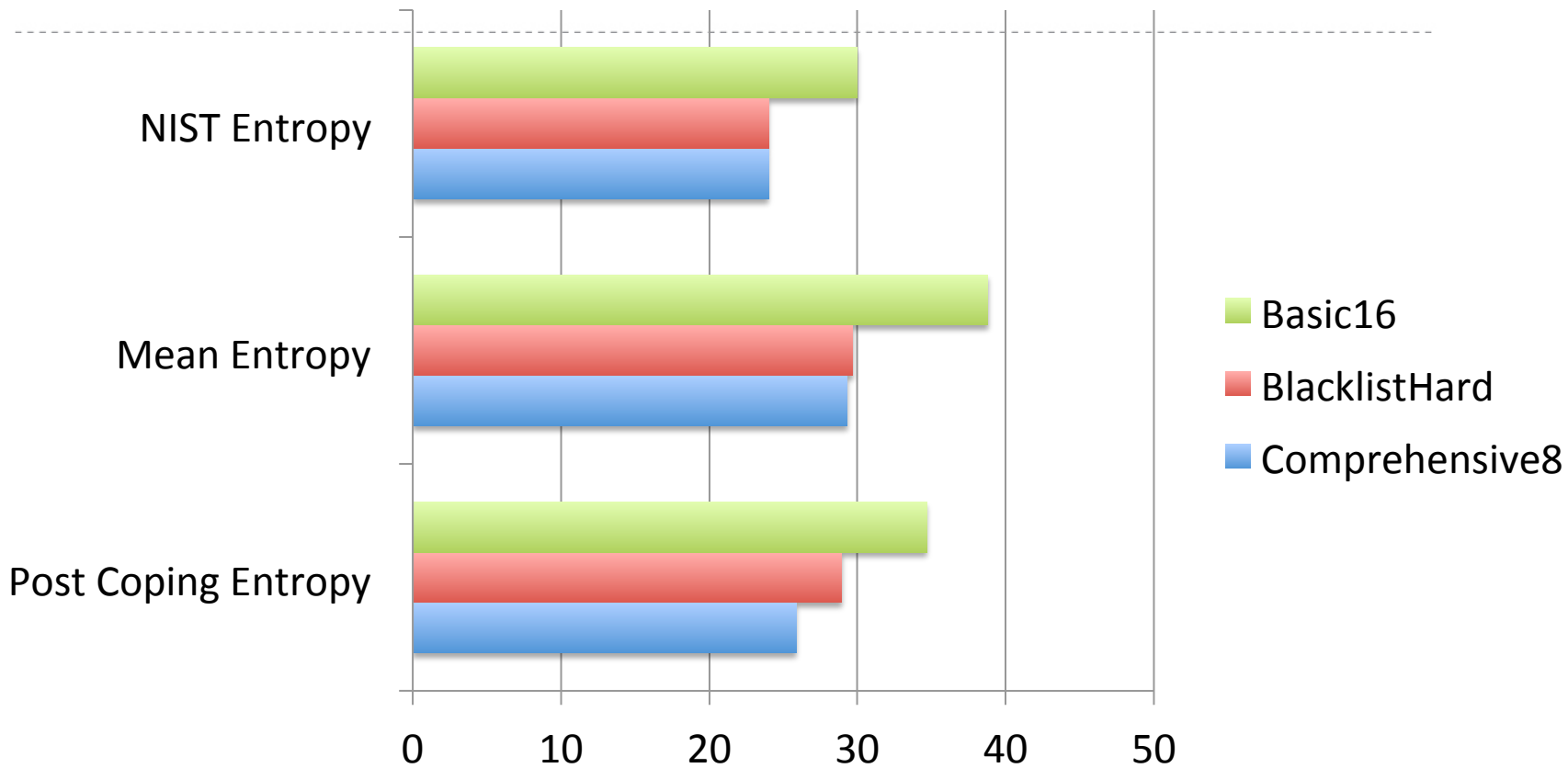
- At least 16 characters long

# PROPOSED DATA ANALYSIS

## CONDUCTED ON PRACTICE PASSWORDS

	Comprehensive8	BlacklistHard	Basic16
N	33	34	37
NIST Entropy	24	24	30
Mean Entropy	29.31	29.69	38.79
Standard Deviation	6.09	3.80	6.52
Confidence Interval (95%)	(27.16, 31.48)	(28.37, 31.02)	(37.91, 42.25)
Post Coping Entropy	25.86	28.93	34.68

# PRACTICE DATA ENTROPY ANALYSIS



Interesting Note: All post coping entropy calculations are greater than the NIST entropy for each policy

# WORK REMAINING

## FINAL REPORT AND PRESENTATION

- Create website
- Collect Data on Mechanical Turk
- Analyze Data collected
- Final Report will be worked on during analysis and completed after analysis of the data
- Final presentation will be given to the Technical Directors and class

QUESTIONS, COMMENTS, OR  
SUGGESTIONS?