Measuring the Security Impacts of Password Policies Using Cognitive Behavioral Agent-Based Modeling

Vijay Kothari [1] Jim Blythe [2] Sean Smith [1] Ross Koppel [3]

[1]Dartmouth College

[2]University of Southern California

[4]University of Pennsylvania

Outline

The Grand Vision

- **Problem:** Those pesky humans make security hard.

The Grand Vision

- **Problem:** Those pesky humans make security hard.
- **Goal:** To create security tools that account for the human.

The Grand Vision

- **Problem:** Those pesky humans make security hard.
- **Goal:** To create security tools that account for the human.
- **Approach:** Human-centric agent-based models.

The Password Problem

- Users make weak passwords.

The Password Problem

- Users make weak passwords.
- So, let's strengthen the password composition policy!

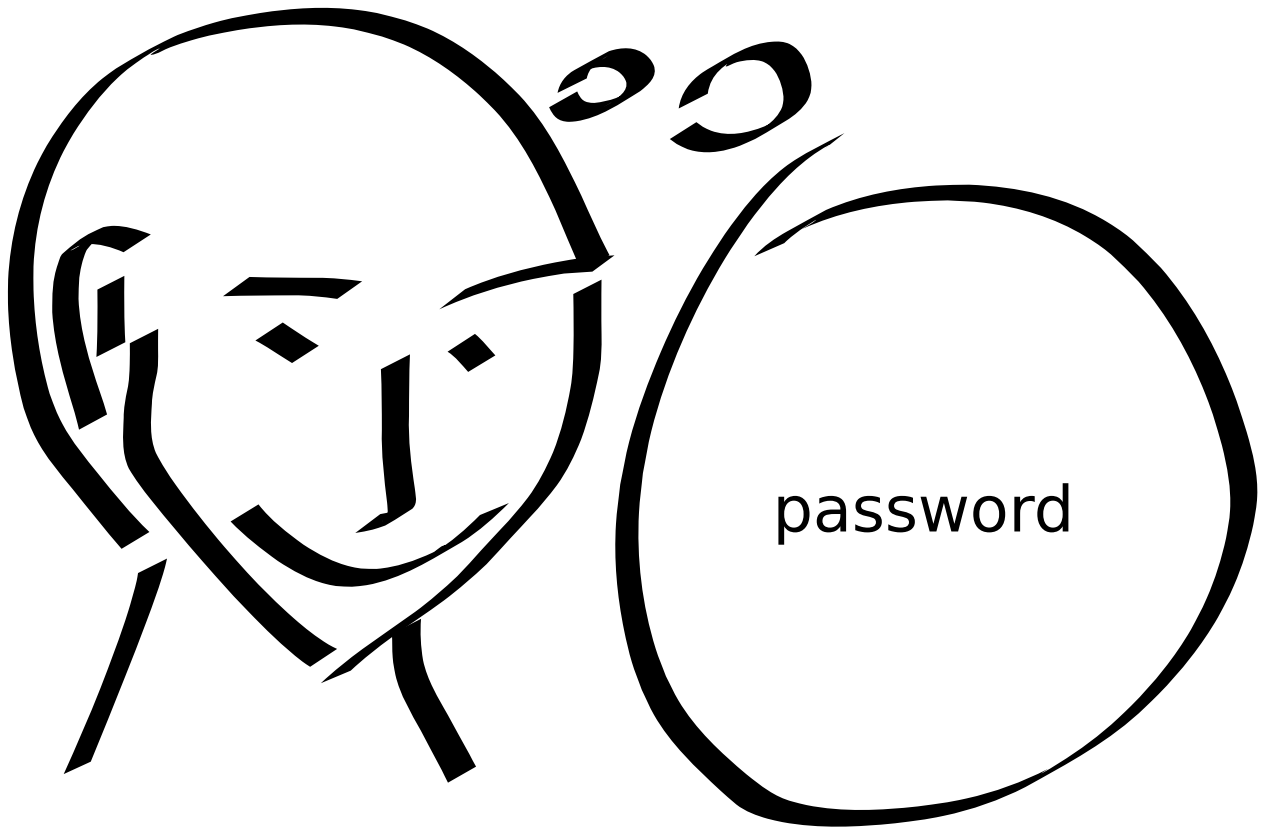
The Password Problem

- Users make weak passwords.
- So, let's strengthen the password composition policy!

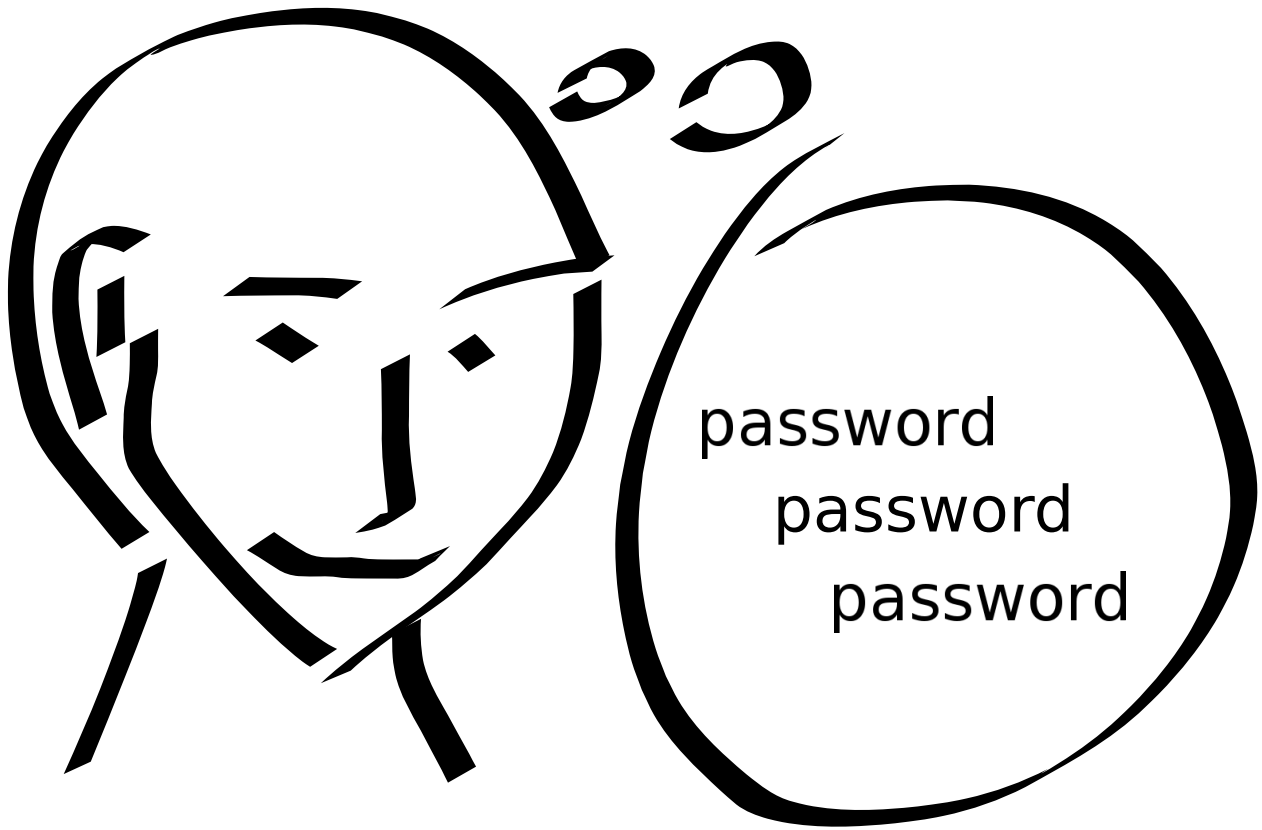
1. The password must be **exactly** 8 characters long.
2. It must contain **at least** one letter, one number, and one special character.
3. The **only** special characters allowed are: @ # $
4. A special character must **not** be located in the first or last position.
5. Two of the same characters sitting next to each other are considered to be a "set." No "sets" are allowed.
6. Avoid using names, such as your name, user ID, or the name of your company or employer.
7. Other words that cannot be used are Texas, child, and the months of the year.
8. A new password cannot be too similar to the previous password.
    a. Example: previous password - abc#1234, acceptable new password - acb$1243
    b. Characters in the first, second, and third positions cannot be identical. (abc*****)
    c. Characters in the second, third, and fourth positions cannot be identical. (*bc#****)
    d. Characters in the sixth, seventh, and eighth positions cannot be identical. (*****234)
9. A password can be changed voluntarily (no Help Desk assistance needed) once in a 15-day period. If needed, the Help Desk can reset the password at any time.
10. The previous 8 passwords cannot be reused.

source: `http://kottke.org/12/06/the-worlds-worst-password-requirements-list`

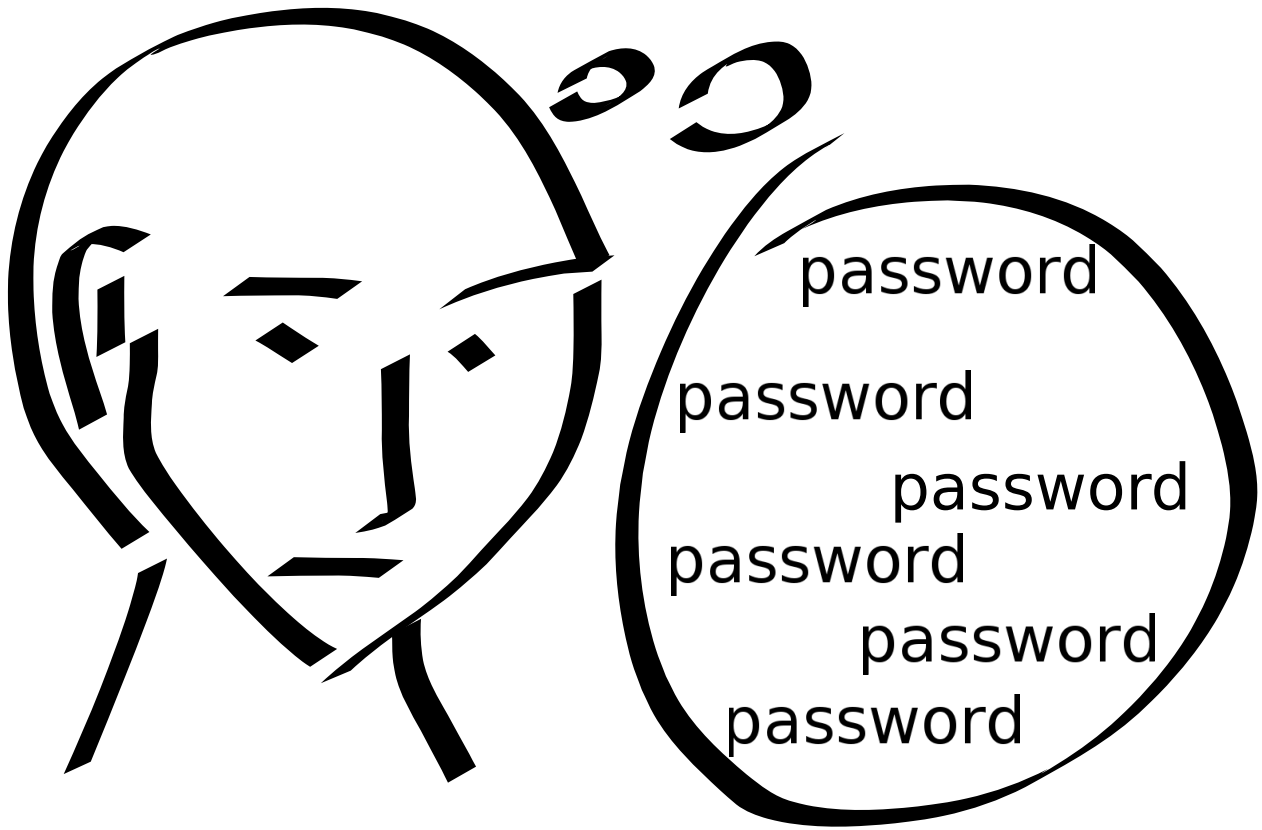
The Password Problem



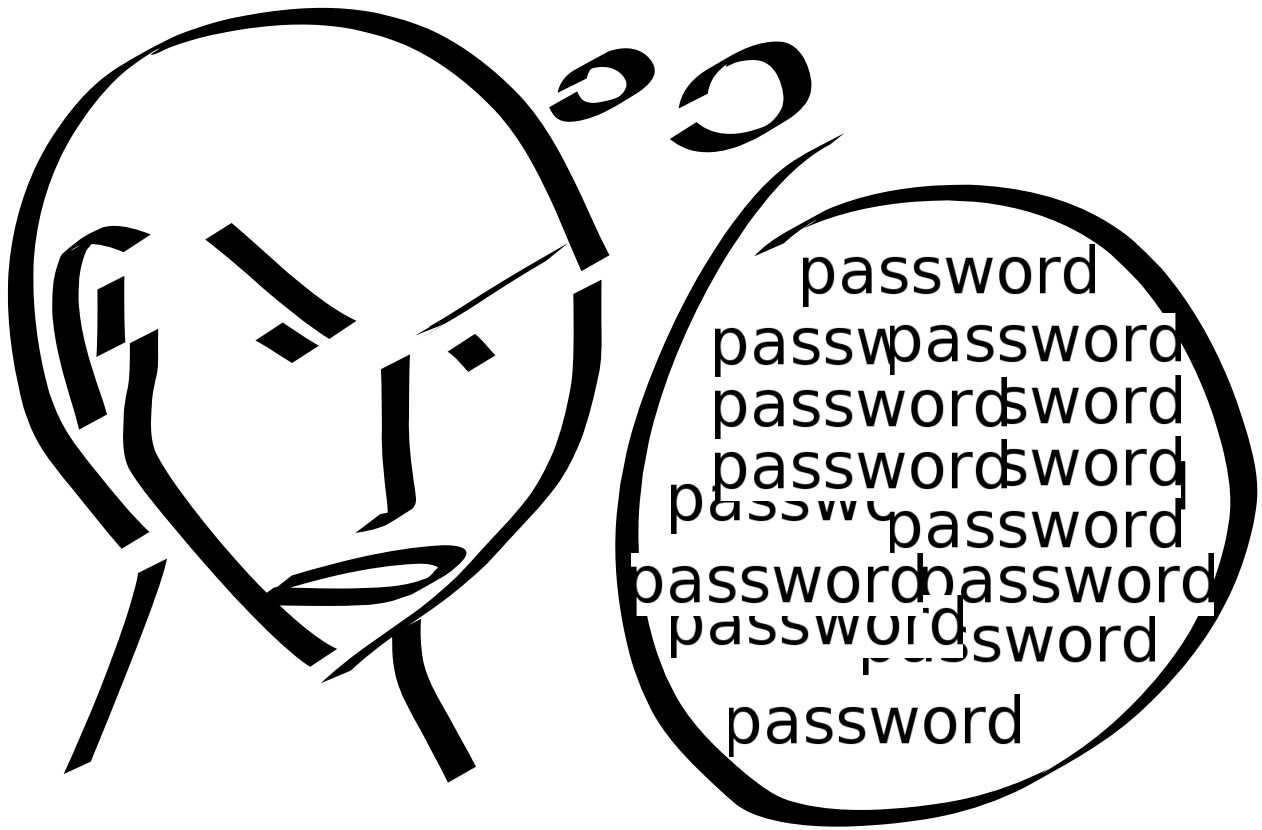
The Password Problem



The Password Problem



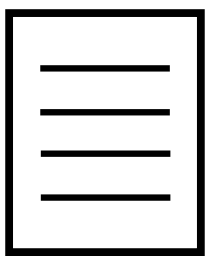
The Password Problem



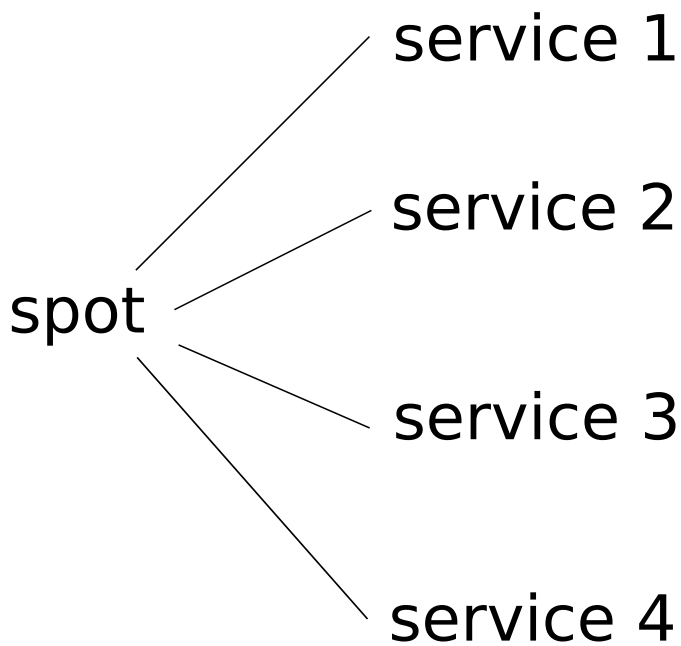
The Password Problem

bank
username:
bob

password:
b47m4n



passwords.txt



The Password Problem

- Can we stop circumvention?

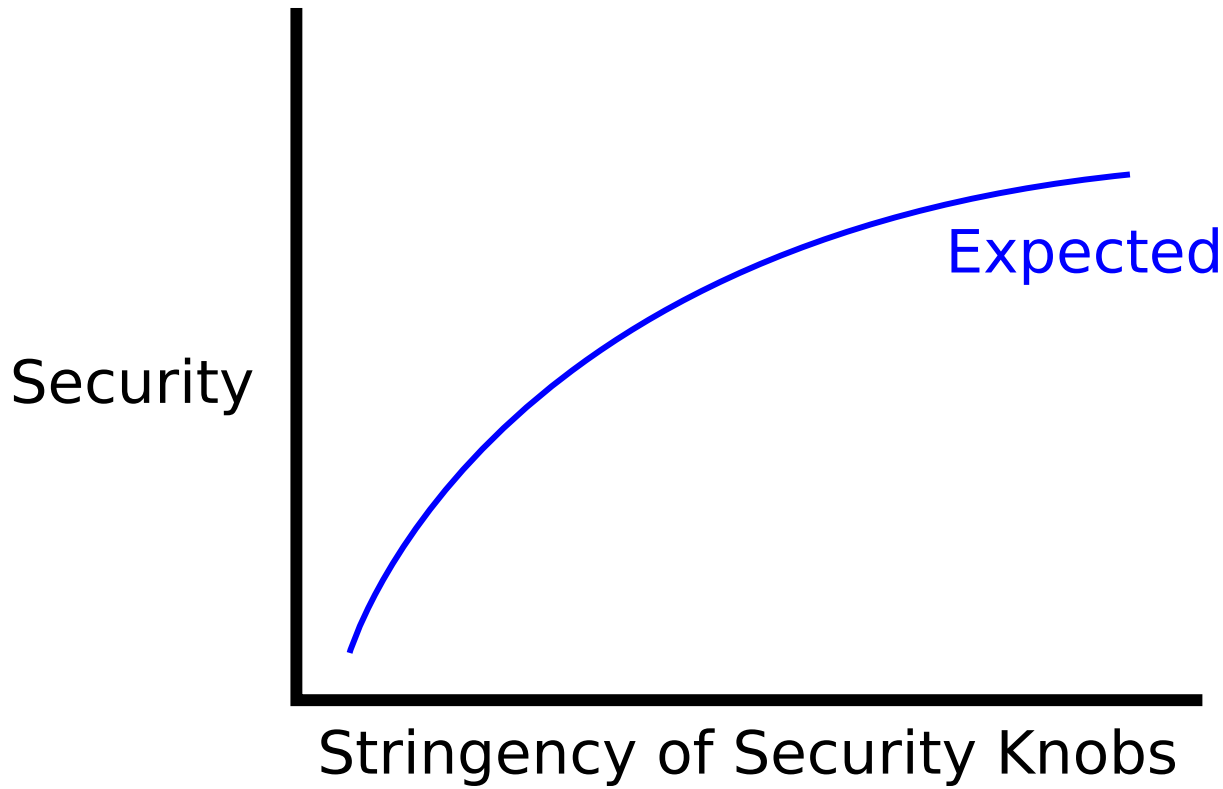
The Password Problem

- Can we stop circumvention?
- Can we set better password policies?

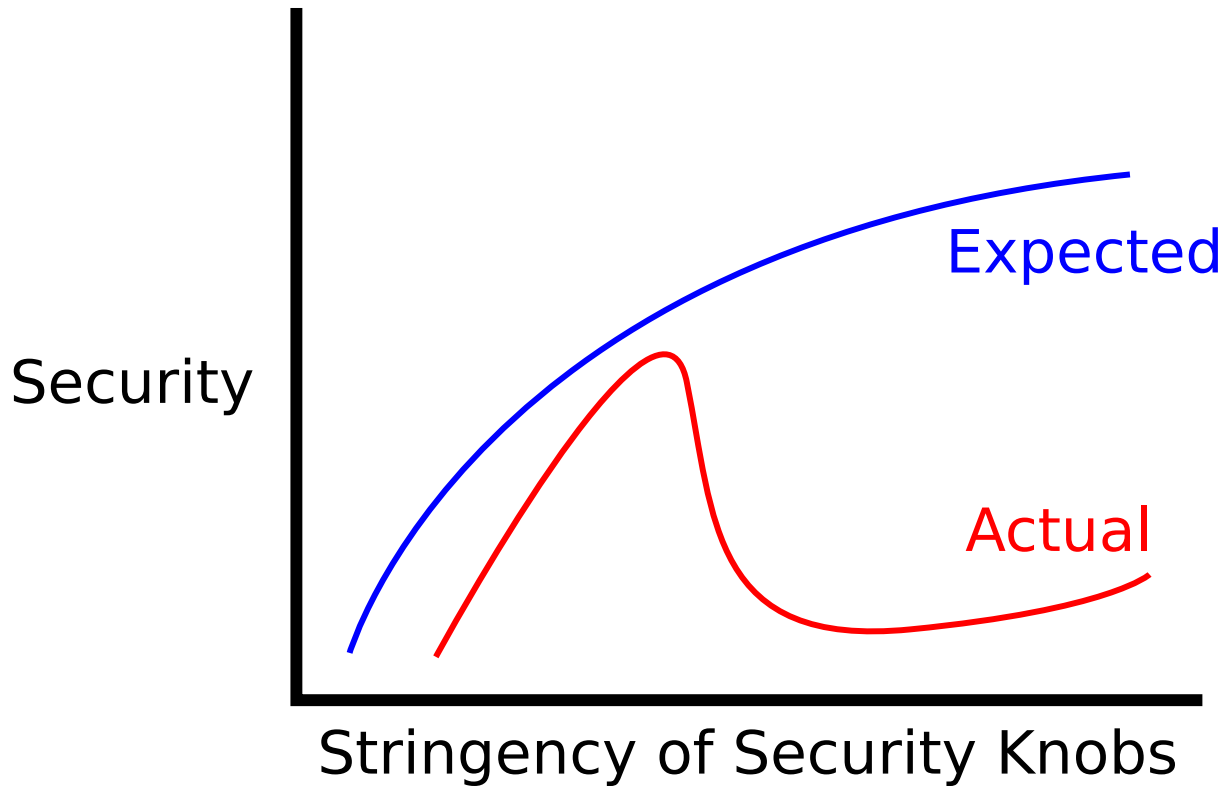
The Password Problem

- Can we stop circumvention?
- Can we set better password policies?
- How do we choose these policies?

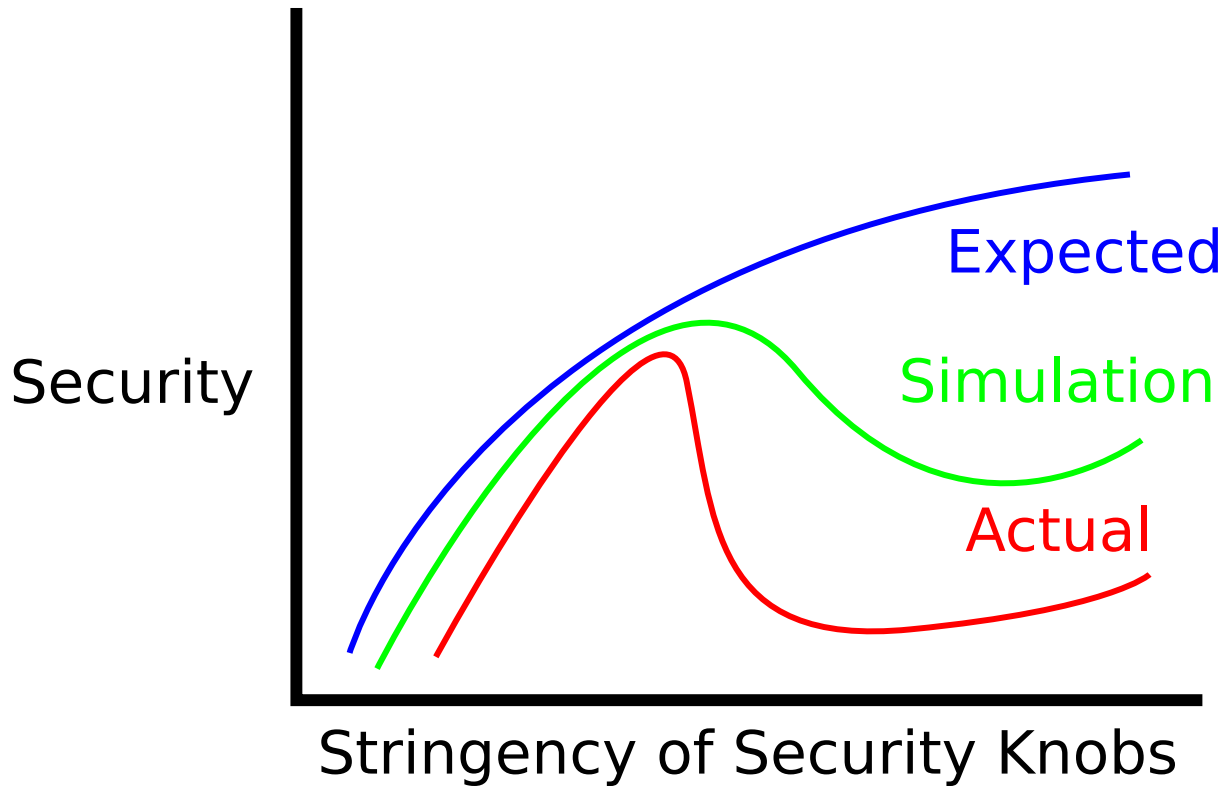
Agent-Based Simulations for Security



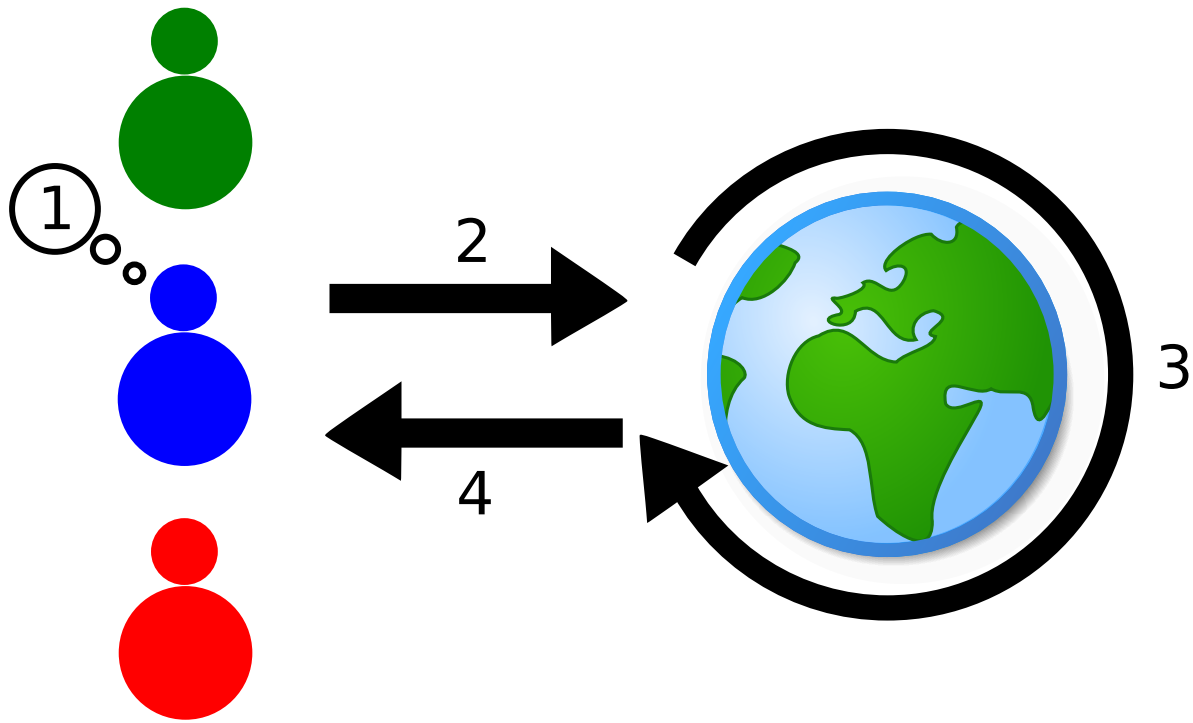
Agent-Based Simulations for Security



Agent-Based Simulations for Security



Bird's Eye View of DASH



source for earth image: `http://commons.wikimedia.org/wiki/File:Ambox_globe.svg`

References:
1. A Dual-Process Cognitive Model for Testing Resilient Control Systems (Jim Blythe)
2. Implementing Models (Jim Blythe and Jean Camp)

DASHWords - Overview

- Agents:
  - create accounts
  - sign in to accounts
  - sign out of accounts

DASHWords - Overview

- Agents:
  - create accounts
  - sign in to accounts
  - sign out of accounts
- They also circumvent.

DASHWords - Overview

- Agents:
  - create accounts
  - sign in to accounts
  - sign out of accounts
- They also circumvent.
- Key underlying models:
  - cognitive burden
  - password recall
  - attack threats

Modeling Cognitive Burden:

- Users can't cope with passwords.

Modeling Cognitive Burden:

- Users can't cope with passwords.
- So, they circumvent.

Modeling Cognitive Burden:

- Users can't cope with passwords.
- So, they circumvent.
- Can we model cognitive burden?

Modeling Cognitive Burden: Levenshtein Distance

- $Lev(S_1, S_2)$: minimum number of edits to convert S_1 into S_2.

Modeling Cognitive Burden: Levenshtein Distance

- $Lev(S_1, S_2)$: minimum number of edits to convert S_1 into S_2.
  Example 1: $Lev(pass, p4sS)$?

Modeling Cognitive Burden: Levenshtein Distance

- $Lev(S_1, S_2)$: minimum number of edits to convert S_1 into S_2.
  Example 1: $Lev(pass, p4sS)$?
  - $pass \rightarrow p4ss \rightarrow p4sS$

Modeling Cognitive Burden: Levenshtein Distance

- $Lev(S_1, S_2)$: minimum number of edits to convert S_1 into S_2.
  Example 1: $Lev(pass, p4sS)$?
  - $pass \rightarrow p4ss \rightarrow p4sS$
  - $Lev(pass, p4sS) = 2$

Modeling Cognitive Burden: Levenshtein Distance

- $Lev(S_1, S_2)$: minimum number of edits to convert S_1 into S_2.
  Example 1: $Lev(pass, p4sS)$?
  - $pass \rightarrow p4ss \rightarrow p4sS$
  - $Lev(pass, p4sS) = 2$
- Example 2: $Lev(\epsilon, pass)$?

Modeling Cognitive Burden: Levenshtein Distance

- $Lev(S_1, S_2)$: minimum number of edits to convert S_1 into S_2.
  Example 1: $Lev(pass, p4sS)$?
  - $pass \rightarrow p4ss \rightarrow p4sS$
  - $Lev(pass, p4sS) = 2$
- Example 2: $Lev(\epsilon, pass)$?
  - $\epsilon \rightarrow p \rightarrow pa \rightarrow pas \rightarrow pass$

Modeling Cognitive Burden: Levenshtein Distance

- $Lev(S_1, S_2)$: minimum number of edits to convert S_1 into S_2.
  Example 1: $Lev(pass, p4sS)$?
  - $pass \rightarrow p4ss \rightarrow p4sS$
  - $Lev(pass, p4sS) = 2$
- Example 2: $Lev(\epsilon, pass)$?
  - $\epsilon \rightarrow p \rightarrow pa \rightarrow pas \rightarrow pass$
  - $Lev(\epsilon, pass) = 4$

Modeling Cognitive Burden: Levenshtein Set Measure

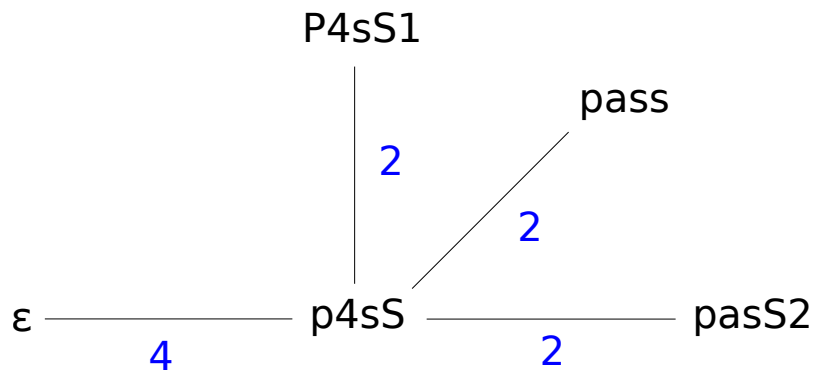
- Let $L(S)$ be the weight of a MST with vertex set $S \cup \{\epsilon\}$.

Modeling Cognitive Burden: Levenshtein Set Measure

- Let $L(S)$ be the weight of a MST with vertex set $S \cup \{\epsilon\}$.
- Suppose $S = \{\epsilon, pass, p4sS, P4sS1, pasS2\}$.

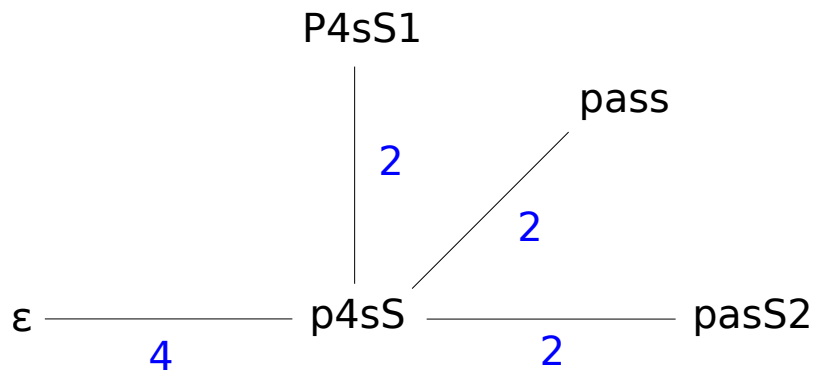
Modeling Cognitive Burden: Levenshtein Set Measure

- Let $L(S)$ be the weight of a MST with vertex set $S \cup \{\epsilon\}$.
- Suppose $S = \{\epsilon, pass, p4sS, P4sS1, pasS2\}$.



Modeling Cognitive Burden: Levenshtein Set Measure

- Let $L(S)$ be the weight of a MST with vertex set $S \cup \{\epsilon\}$.
- Suppose $S = \{\epsilon, pass, p4sS, P4sS1, pasS2\}$.



$$L(S) = 4 + 2 + 2 + 2 = 8$$

Modeling Cognitive Burden: Cognitive Thresholds

- Use Levenshtein set measure for cognitive burden!

Modeling Cognitive Burden: Cognitive Thresholds

- Use Levenshtein set measure for cognitive burden!
- Cognitive burden and circumvention:

Modeling Cognitive Burden: Cognitive Thresholds

- Use Levenshtein set measure for cognitive burden!
- Cognitive burden and circumvention:
  - Password Write Threshold.

Modeling Cognitive Burden: Cognitive Thresholds

- Use Levenshtein set measure for cognitive burden!
- Cognitive burden and circumvention:
  - Password Write Threshold.
  - Password Reuse Threshold.

Modeling Password Beliefs

- Agents have per-service password belief strengths.

Modeling Password Beliefs

- Agents have per-service password belief strengths.
- Belief strengths collectively describe agent password memory.

Modeling Password Beliefs

- Agents have per-service password belief strengths.
- Belief strengths collectively describe agent password memory.
- Agent actions and results affect belief strengths.

Measuring Password Security

- Direct Attack: P_{DA}

Measuring Password Security

- Direct Attack: P_{DA}
- Stolen Password Attack: : P_{SP}

Measuring Password Security

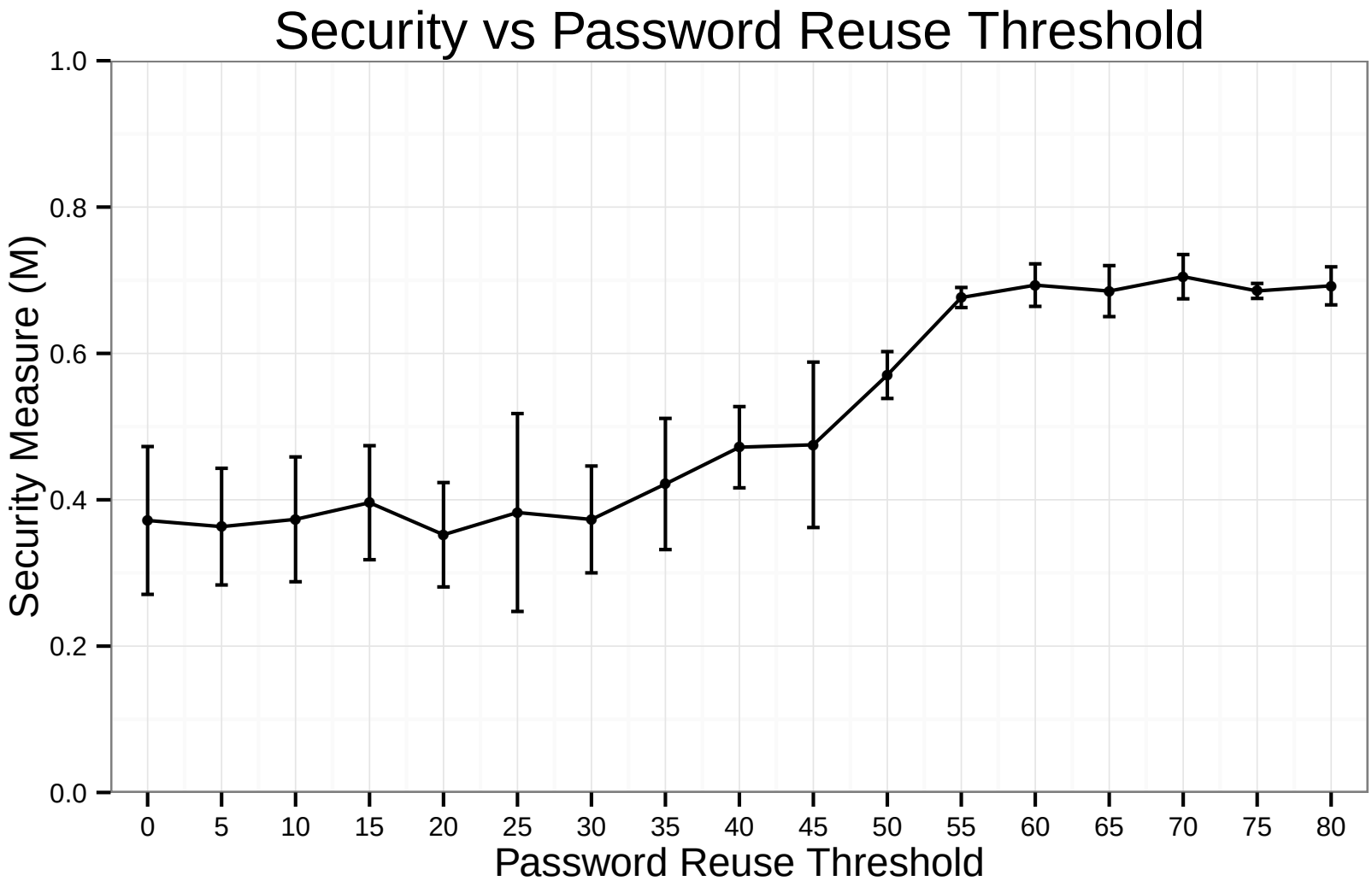
- Direct Attack: P_{DA}
- Stolen Password Attack: : P_{SP}
- Password Reuse Attack: P_{RA}

Measuring Password Security

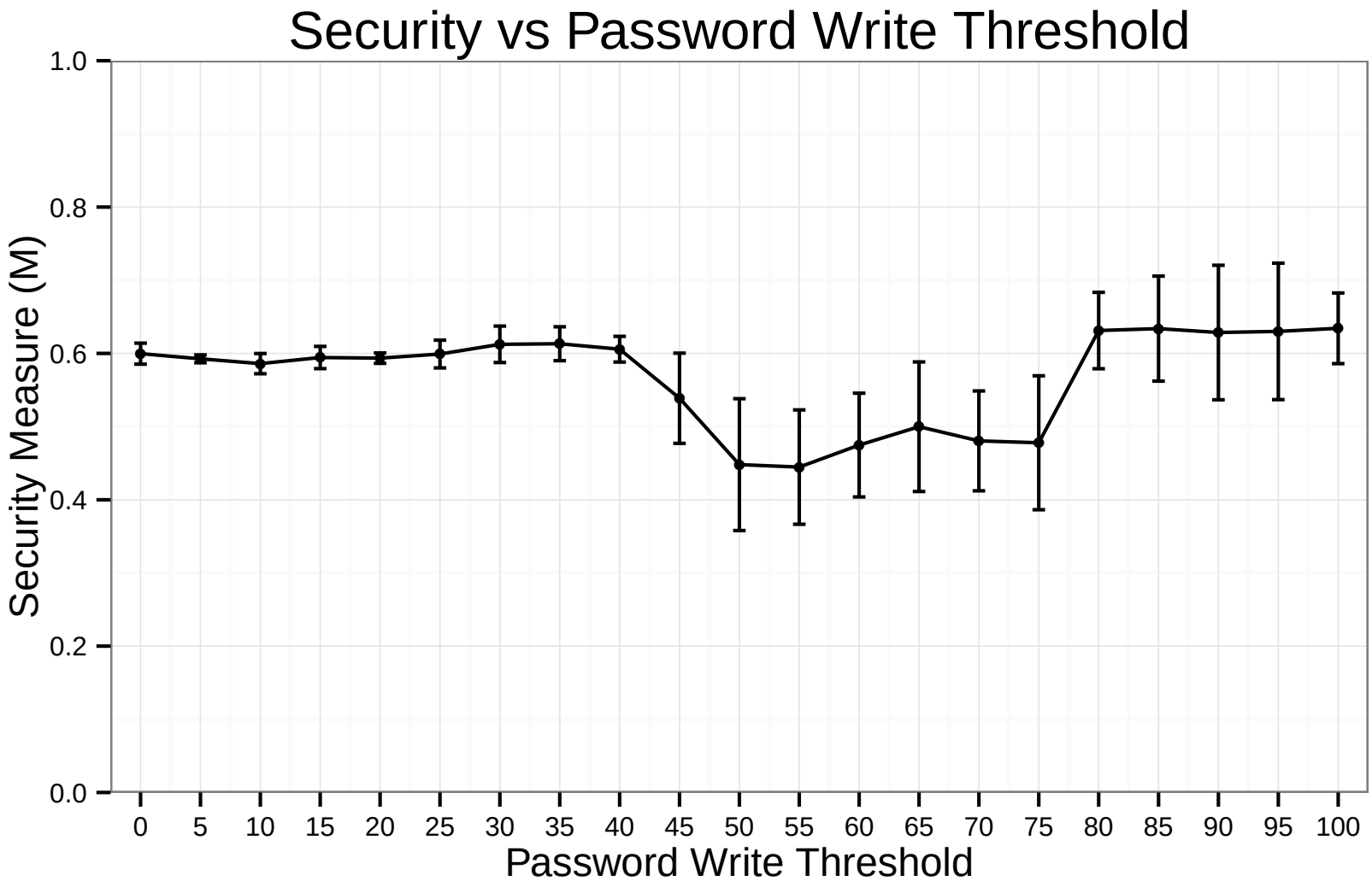
- Direct Attack: P_{DA}
- Stolen Password Attack: : P_{SP}
- Password Reuse Attack: P_{RA}
- Aggregate Security:

$$M = P(SAFE) = (1 - P_{DA}) * (1 - P_{SP}) * (1 - P_{RA})$$

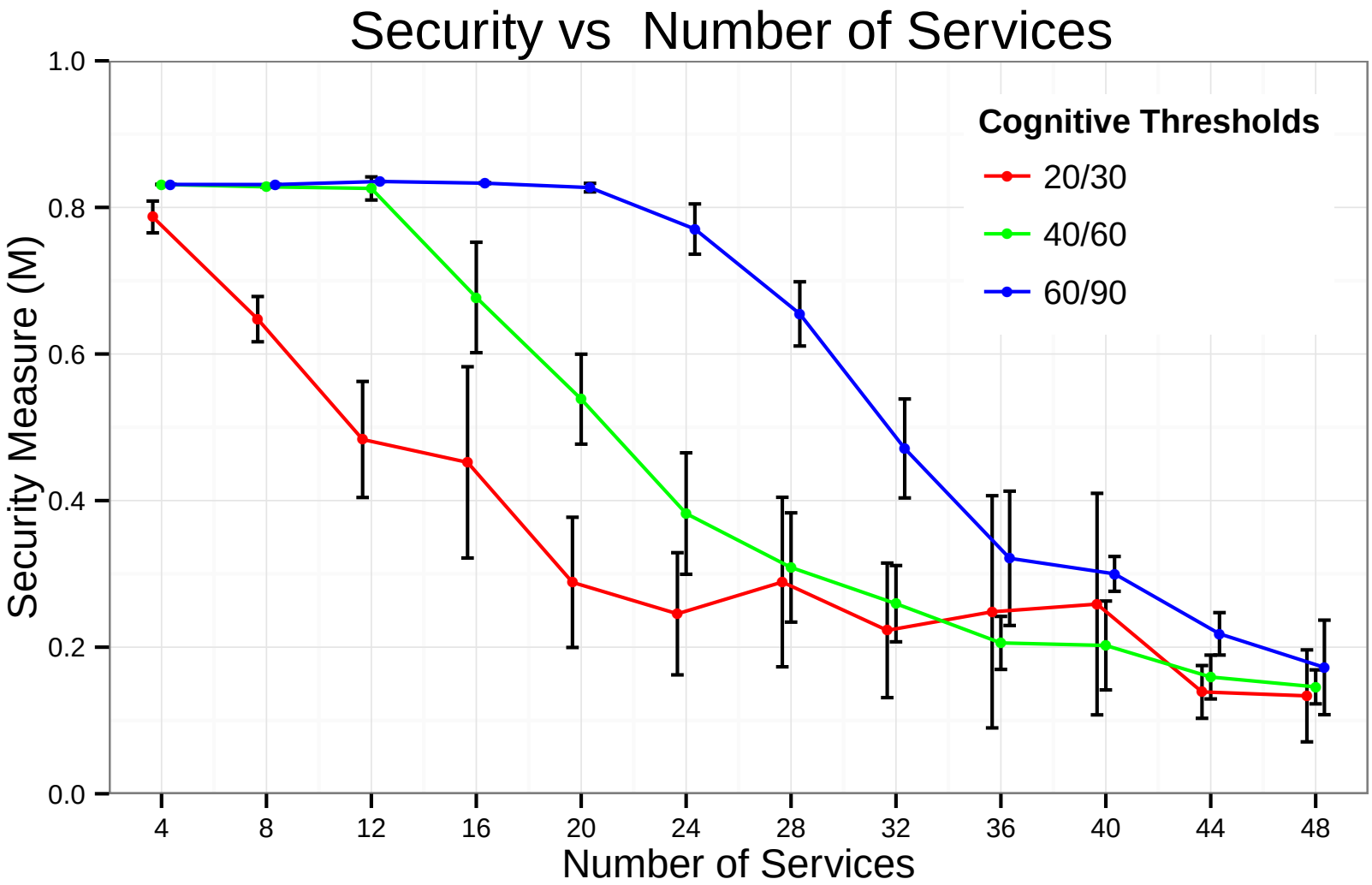
Results - Security vs Password Reuse Threshold



Results - Security vs Password Write Threshold



Results - Security vs Number of Services



Future Work

- Future Password-Related Work:
  - Other circumventions
  - Group dynamics
  - Endorsing circumventions
  - More accurate modeling
  - Validation
- Autologouts
- Other problems?

Conclusion

- Humans circumvent.

Conclusion

- Humans circumvent.
- We must acknowledge and account for circumvention.

Conclusion

- Humans circumvent.
- We must acknowledge and account for circumvention.
- This necessitates better policy tools.

Conclusion

- Humans circumvent.
- We must acknowledge and account for circumvention.
- This necessitates better policy tools.
- Agent-based simulations may help.

Thank you!

Contact Information:

Vijay Kothari: vijayk@cs.dartmouth.edu
Jim Blythe: blythe@isi.edu
Sean Smith: sws@cs.dartmouth.edu
Ross Koppel: rkoppel@sas.upenn.edu