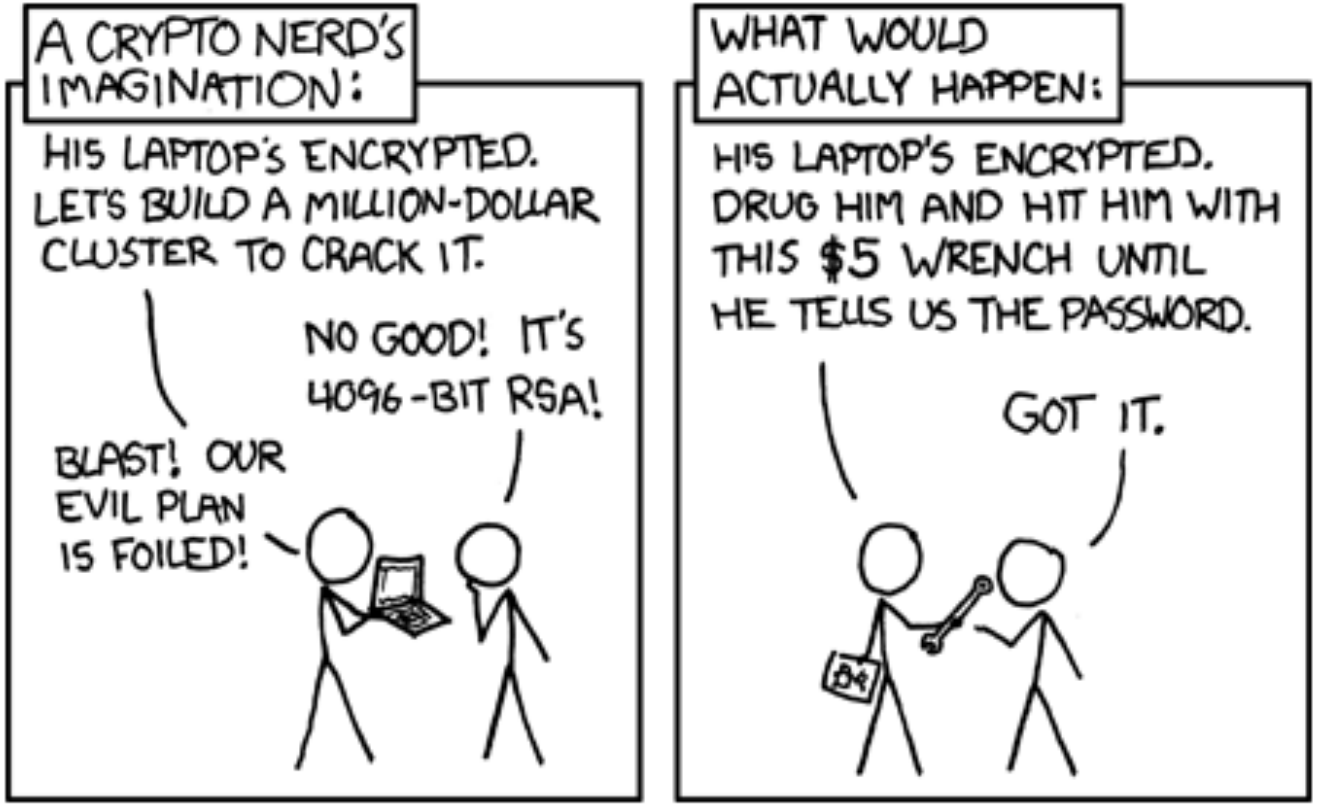
Visualizing Keyboard Pattern Passwords

Dino Schweitzer, Jeff Boleng,
Colin Hughes, Louis Murphy

Oct 2009


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Overview

- Background
- Project Approach
- Collecting Data
- Visualizing
- Results

Background

- Introductory computer security course
- 2-person research projects
  - Complete research process
  - Faculty mentors
  - Work on “real problems”
- Murphy / Hughes team wanted to investigate keyboard patterns

The problem

- Hypothesis that a lot of people use keyboard patterns to meet password rules while creating a memorable key sequence
  - Appear random when look at text
  - Not in dictionaries
  - Easy to remember
- Are such patterns vulnerable to attack?

Sample Password Rules

- The password must be at least 8 characters long.
- The password **must** contain at least:
  - one uppercase and one lowercase alpha character [a-z A-Z];
  - one numeric character [0-9];
  - one special character from this set:
    ` ! @ $ % ^ & * ( ) - _ = + [ ] ; : ' " , < . > / ?
- The password **must not**:
  - contain spaces;
  - begin with an exclamation [!] or a question mark [?];
  - contain your login ID.
- The first 3 characters cannot be the same.
- The sequence of the first 3 characters cannot be in your login ID.
- The first 8 characters cannot be the same as in your previous password.
- Passwords are treated as case sensitive.

Project Approach

- Collect a bunch of passwords
- Analyze for patterns
- Identify common patterns
- Come up with way of using common patterns to attack a password file
- Show proof of concept on a real password file

Collecting Passwords

- Wanted a large sample size
- Ideally, people would not know purpose of samples (or even that they were being collected)
- Also, ideally, have some that know are intended as patterns, versus random ones

Collecting Passwords

- Wanted a large sample size
- Ideally, people would not know purpose of samples (or even that they were being collected)
- Also, ideally, have some that know are intended as patterns, versus random ones

SOLUTION

Our Freshman class!

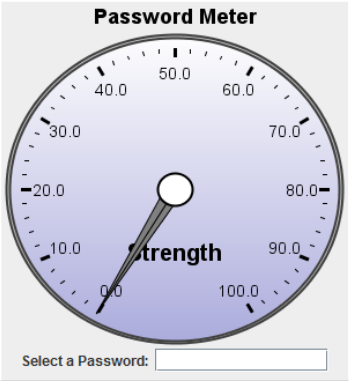
Password WebLab

- Set of 7 web pages designed to teach freshmen about passwords
  - Strength, entropy, common attacks, different types
  - Interactive applets to (hopefully) make more compelling and encourage participation
  - Had them enter random, pattern, passphrases
  - Anonymously collected all passwords for analysis

Screen Shots

Passwords Web Lab

The purpose of the following web pages is to teach you some fundamental concepts about passwords, the most common mechanism used to provide *access control* to computers, services, and resources. We are all familiar with creating them, using them, and trying to remember them for everything from getting into our email account to purchasing the latest online gizmo. These pages will describe different aspects of password strength, selecting passwords, and cracking passwords and give you an opportunity to experiment with different approaches. When asked to choose a password, **YOU SHOULD NEVER ENTER ONE OF YOUR CURRENT PASSWORDS**.



Introduction

Here is an approximation of how weak or strong your password may be based on length and characters chosen.

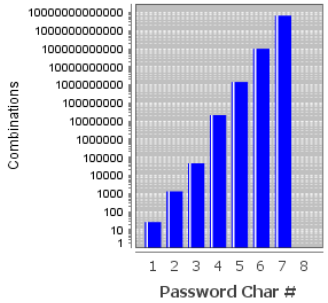
Go ahead and enter a password. Try something simple, and then something more complex. The length and complexity (numbers, uppercase, lowercase, special characters) will affect how "strong" the password is, that is, how difficult it will be to break.

Passwords Web Lab

Remember, when asked to choose a password for demonstration purposes,

YOU SHOULD NEVER ENTER ONE OF YOUR CURRENT PASSWORDS.

Possible Combinations



Select a Password: o0o-i0i

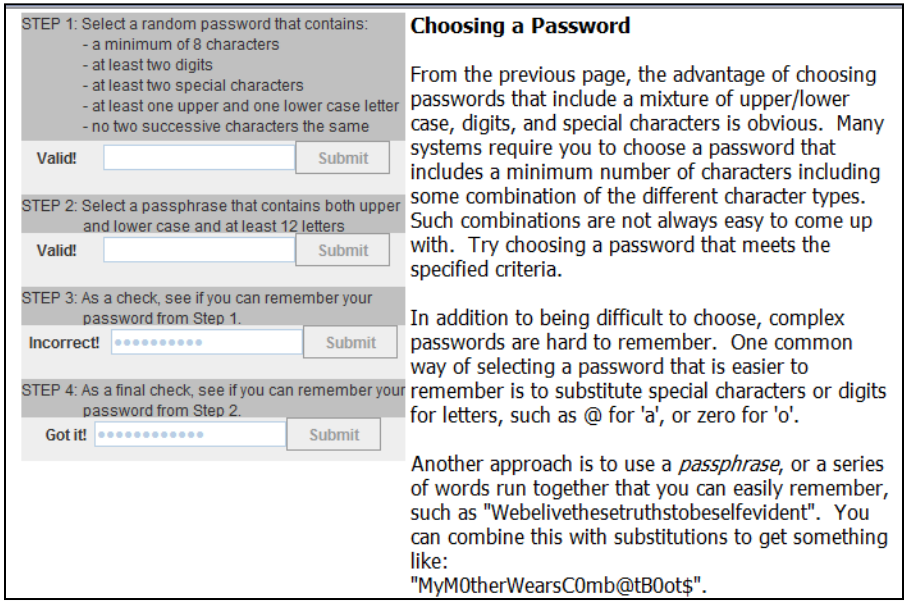
Time to Guess: 2.1 years

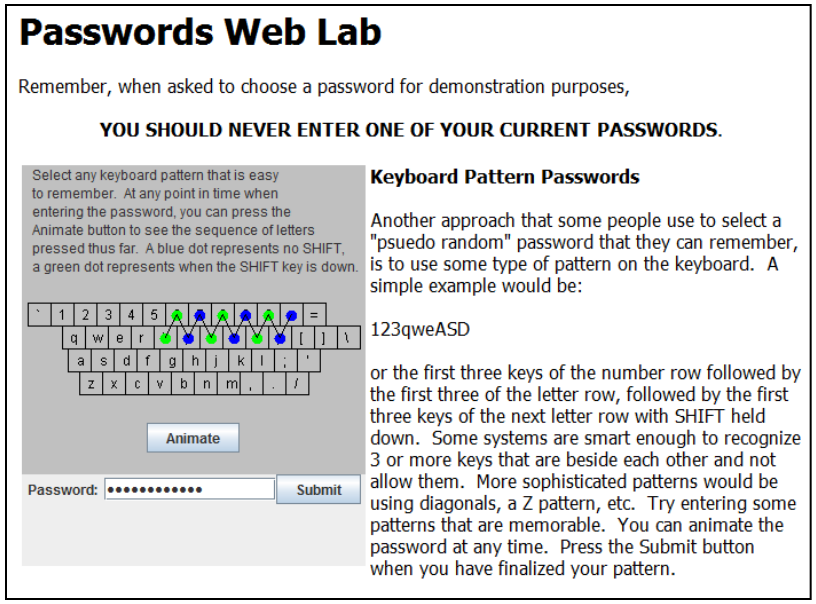
Entropy

One method of measuring the "strength" of a password is called the *entropy,* or degree of randomness, of it. This value is a function of the number of possible combinations of passwords which is calculated from the length of the password and the total number of possible values per password character. For example, if your password is all digits, there are only 10 possible values per character. If your all-digit password is 2 characters, then there are only 100 possible password combinations (00-99). If you use all lowercase letters and digits, there are 36 possible values per character. If you utilize the entire keyboard including upper, lower, digits, and special characters, there are 94 possible values.

The **logarithmic** graph shows the total number of combinations for your password (up to 8 characters). In addition, at the **conservative** rate of being able to guess 100,000 passwords per

Screen Shots



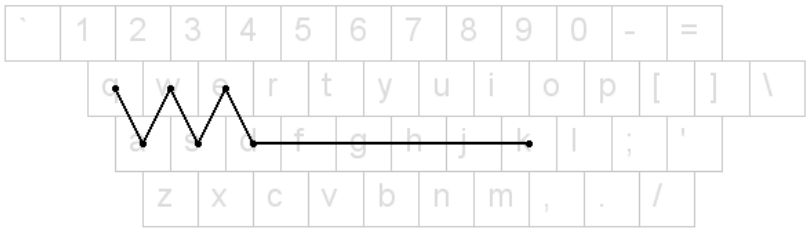


Collected Data

- 161 distinct users
- Over 500 “random” passwords
- Over 250 “pattern” passwords
- Based on collected passwords, it was obvious students did not know they were being saved

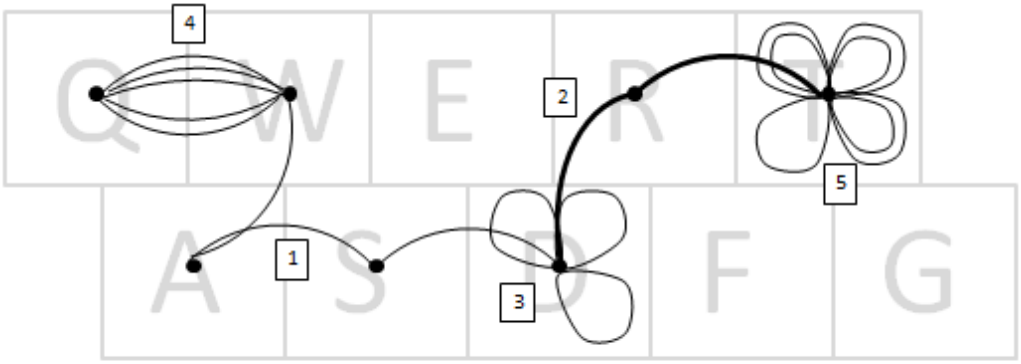
Visualizing Patterns

- First attempt to simply draw lines between characters on keyboard
  - Some patterns obvious
  - Did not show same key hits
  - Could not tell when sequence repeated
  - Could not tell when shift key pressed
- Also played with animating sequence
  - Hard to compare multiple passwords for common patterns



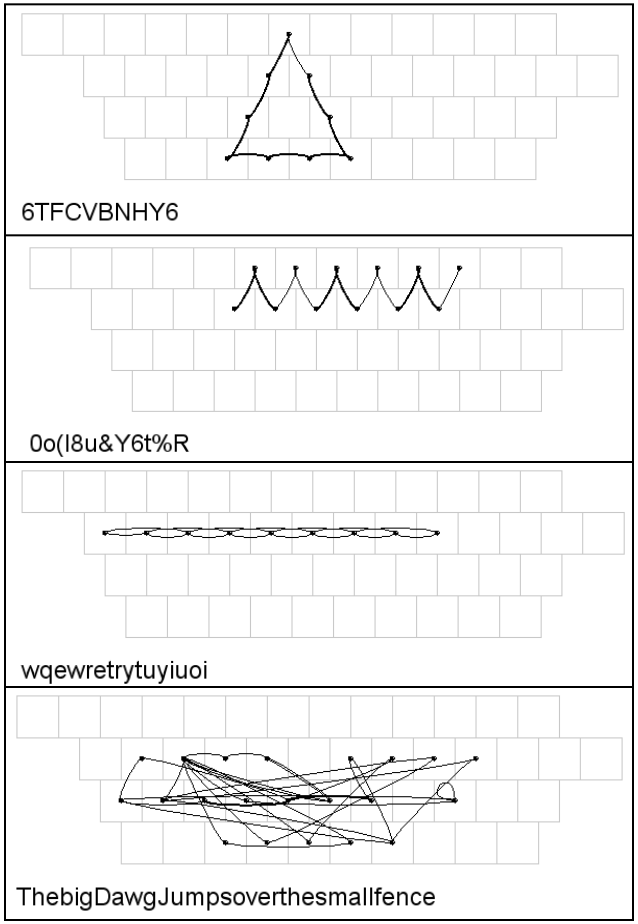
Drawing Rules

1. Connect keys with an arc
2. Increase the weight for shift
3. Loops for same key
4. Repetition uses offset arcs
5. Repetition of same key more than 4, offset loops
6. Arcs drawn in clockwise order

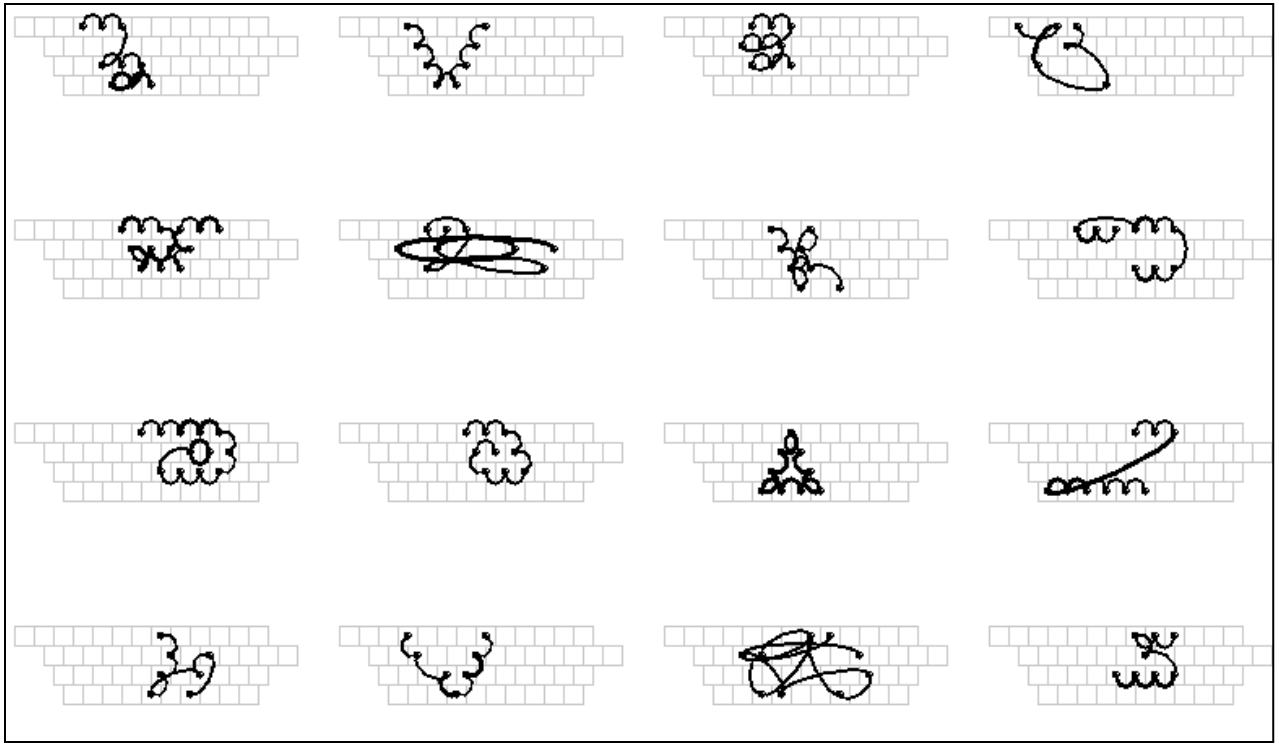


Password: qwqwqwasddddRTttttttt

Samples from Data



Looking for Common Patterns

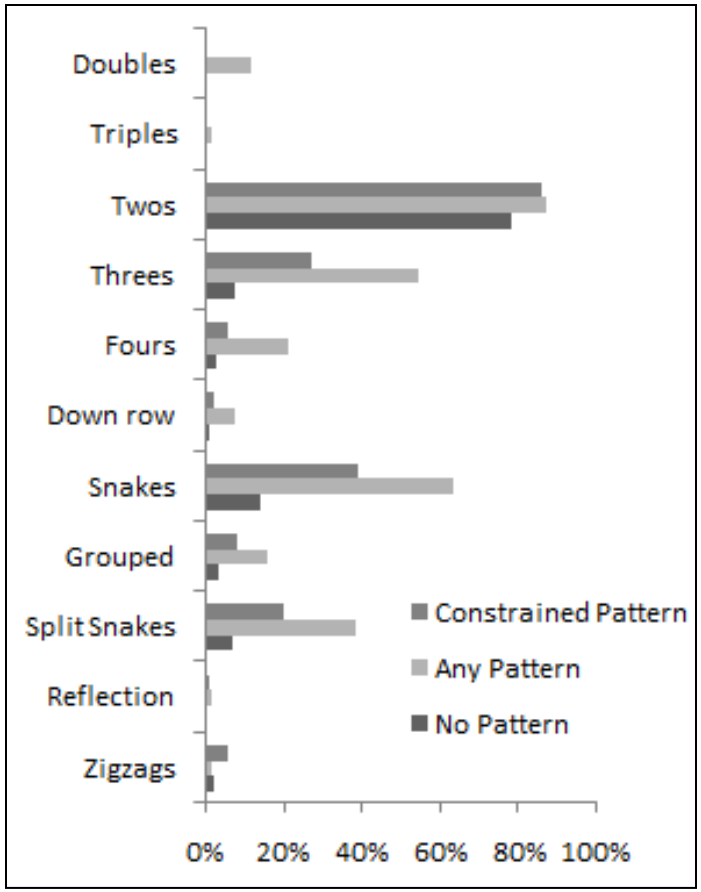


Identified Patterns

Pattern Name	Description
Doubles	Same key pressed twice in succession
Triples	Same key pressed three times in succession
Twos	Two keys in a continuous line
Threes	Sets of three keys in a continuous line
Fours	Sets of four keys in a continuous line
Down-the-row	Five or more keys in one row
Snake	Sequence of contiguous keys
Grouped 2/3/4's	Sets of 2's, 3's, 4's offset by row or diagonal
Split Snake	Two discontinuous snake parts
Reflected	Sequence of mirrored keystrokes
Zig-zag	Alternating contiguous keys from two rows

Pattern Frequency

- Based on visually identified common patterns
  - Programmatically checked collected data for frequency
- Some interesting results
  - "Threes" occur often in patterns, seldom in random
  - Doubles and Triples rare
  - ~20% random passwords had some type pattern



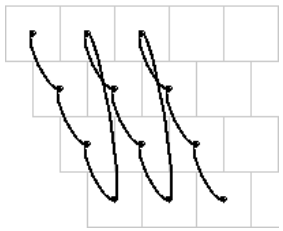
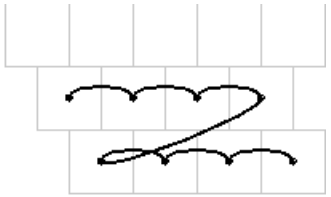
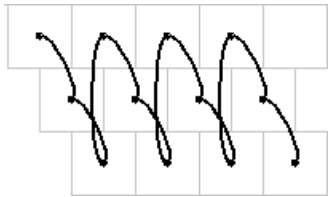
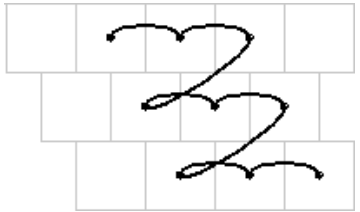
Attacking Patterns

- Decided to attack “Grouped 2s/3s/4s”
  - Occurred in 15% of patterns

- Basic approach
  - Develop rules to generate all possible 2s/3s/4s patterns
  - Create a dictionary of patterns
  - Attack using a standard dictionary approach

Creating Passwords

- Used following rules to generate
  - Meets locally enforced complexity rules
  - Password parts (individual sets of 2, 3, or 4 keys in a row) go in the same direction
  - Password parts are the same length
  - Password parts are either all shifted up, or all not
  - Password parts go left to right, or top to bottom
  - Password parts are only 1 space off on the keyboard
- Resulting dictionary had ~500,000 entries

Testing Dictionary

- Wanted to test against “live” password file
- Difficulty convincing IT group to provide real file (even an old one)
- Finally, obtained small production file containing 11 “strong” password hashes
  - John the Ripper did not discover any of them in 18 hours of run time
  - Pattern dictionary discovered 2 in under 1 second

Conclusions

- Keyboard pattern passwords common
- Common pattern elements prevalent
- Visualization an effective means to identify common pattern elements
- Keyboard pattern passwords susceptible to detection
  - Can create customized tool to check common patterns
  - Treat common pattern elements as “words” to create new dictionaries

Visualizing Keyboard Pattern Passwords

Dino Schweitzer, Jeff Boleng,
Colin Hughes, Louis Murphy

Oct 2009