Usability Research in Support Of Cyber-Security: A Password Policy Taxonomy

Kevin Killourhy
Visualization & Usability Group
Information Access Division
Information Technology Laboratory
Comprehensive National Cyber-Security Initiative: Research and Development
Usability Research Goal:

To enable policy makers to make better decisions
View of solution space of the security and usability equation

- Trivial security solution
- Optimum acceptable usability/security solution
- Each point (solution) has a security level and a usability level
- Policy constrains solution space
- Ideally policy will permit the best solution
- Trivial usability solution
Password Policy Quiz

- What are the minimum length and maximum lifetime?
- Are special characters required?
- Which special characters are allowed?
- Is white-space allowed?
- Are you allowed to write it down?

Workplace password policies involve much more than length and lifetime.
Password policies cause confusion

- Users rarely understand them
- Users are governed by multiple policies at work, through financial institutions, and for other online activities.
- The number of policies, ambiguities in them, and discrepancies among them are a cognitive burden.

So...

- Users are forced to choose weak passwords or write them down.
- Policy violations become routine
- Password policy security goals are not met
Can you follow this policy?

Policy from a Federal Agency:

Passwords contain a combination of letters, numbers, and at least one special character

- What constitutes a special character anyway?

- Is the following a legal password:
  - `password2%` (letters, number, and specials) ?
  - `password%` (letters and specials) ?
  - `Password%` (upper-case and lower-case letters and specials) ?
  - `|*@$%^()%&` (all specials) ?
Password specifications as Policies

- Policies regulate behavior (or they try to).

  For instance:
  - Users must not store passwords in writing anywhere.
  - Users must create passwords with a character in the set of numbers.
  - Users must not create passwords in the set of dictionary words.

- But they are not written in clear and unambiguous language.
Policies vary dramatically both in length and language.
Goal

Develop a effective approach for studying password policies.

• Specifically, develop a password policy language that enables us to
  (1) evaluate and compare policies, and
  (2) assess how policy rules affect user behavior and security.

• Approach:
  – Develop a taxonomy of policy rules
  – Collect a corpus of representative policies
  – Analyze the corpus using its taxonomic structure
Develop a Taxonomy

Reduce policies to an unambiguous language:

Benefits of a formal (EBNF) grammar:
- Specific statements can be pinpointed for discussion.
- What is allowed, forbidden, and ambiguous is explicit.
- Language differences no longer prevent comparisons. *(Clarity first)*

Users must change passwords immediately if compromised.
Users must not create passwords repeated 5 or more times.
Users must create passwords with length greater than or equal to 8 characters.
Users must not create passwords an outside system.
Users must not create passwords character repeated 5 or more times.
Users must not create passwords years of passwords.
Benefits of a formal (EBNF) grammar:

- What is allowed, forbidden, and ambiguous is explicit.
- Specific statements can be pinpointed for discussion.
- Language differences no longer prevent comparisons. (Clarity first)
Apply Taxonomy to a Corpus

- Corporate and government policies of primary interest (22)
- Password-protected general websites policies included (19)
How many different rules?
- 41 policies
- 155 unique rules
- 449 total rules
A visual representation of the corpus
A visual representation of the corpus
Policy exploration and visualization
Depiction of a password policy
Users must create passwords with length greater than or equal to 8 characters.
Comparing two policies

Users should not communicate passwords by local-area network without encryption.
A tool for password policy analysis

- General statistics:
  - Are any two policies the same?
  - What rules appear frequently?
  - How often are policies ambiguous or contradictory?

- Broader questions:
  - Which rules constitute best practices?
  - Which rules require user cooperation?
  - What rules affect usability? What rules affect security? How?
Some preliminary results

- Are any two policies the same?
  - No (they are like snowflakes).
  - NIST (28) and the Census Bureau (22) share 14.
  - DoC (28) shares 12 with NIST and 8 with Census.
Some preliminary results

• What rules appear frequently?
  • Users must create passwords with length greater than or equal to 8 characters. (23)
  • Users must not communicate passwords to anyone. (15)
  • Users must change passwords immediately if compromised. (10)
  • Users must not create passwords with a substring in the set of dictionary words. (10)

• 73 rules appear only once.
Some preliminary results

• How often are policies ambiguous or contradictory?
  • Rules were flagged as ambiguous if they...
    • Concerned special characters without defining them,
    • Concerned “letters” without specifying case,
    • Concerned vague prohibitions on “patterns”
  • 34/41 policies (83%) contain an ambiguous rule.
Basic findings

- A typical policy imposes 8—10 rules on a user.
- Each policy introduces an average of 1—2 unique rules.
- Nearly every policy had ill-formed requirements.
- Users with multiple passwords will not be able to keep all the requirements straight.
Next Steps

- Attach security rationales to rules and regions.
- Attach usability concerns and experimental results.
- Translate policies to find disagreement or misinterpretation.
- Explore current practices and establish best practices.
- Put policies into plain language.
- Thank you!

26