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

Kevin Killourhy
Visualization & Usability Group
Information Access Division
Information Technology Laboratory

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

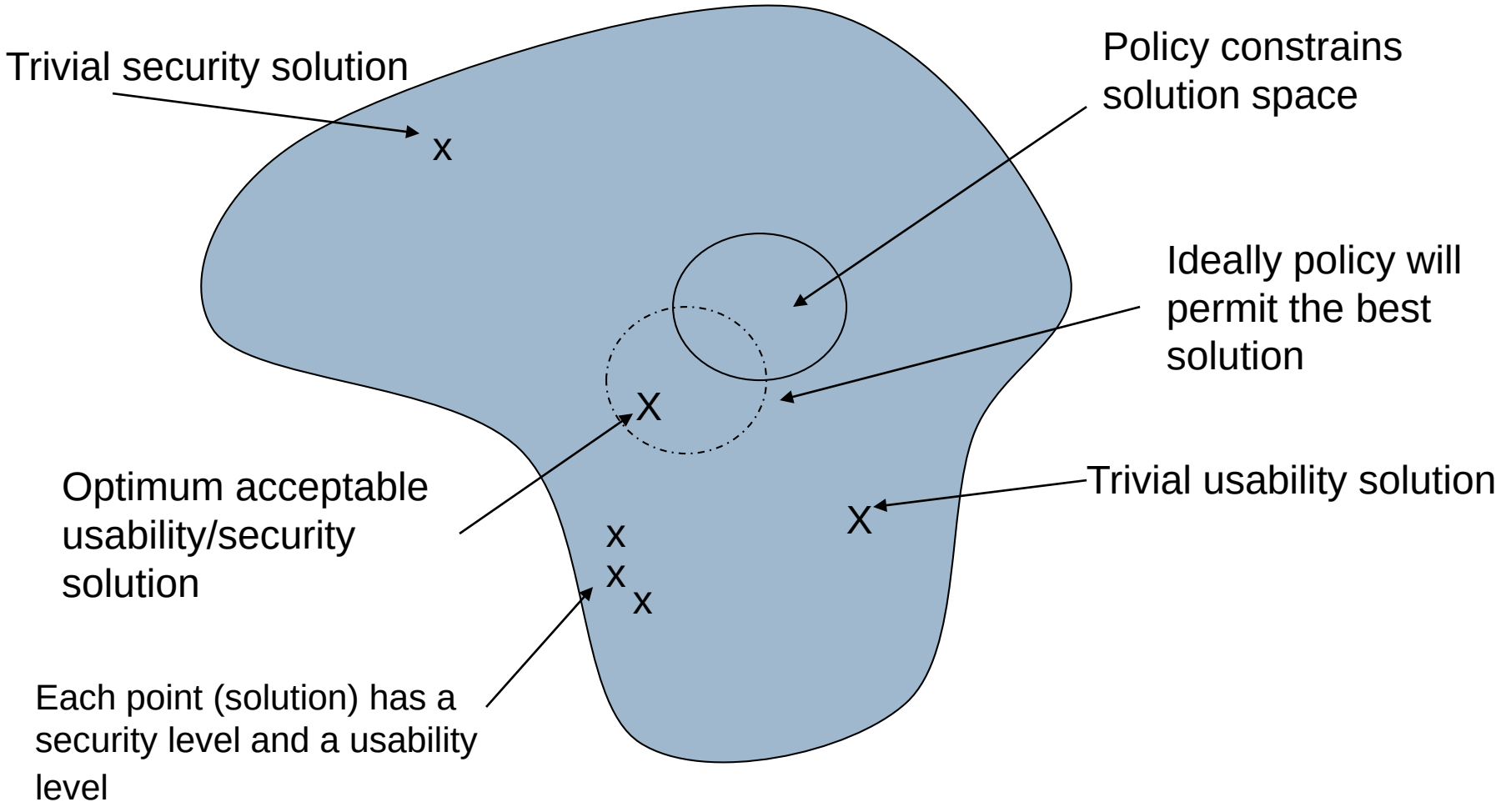
Comprehensive National Cyber-Security Initiative:

- Research and Development

Usability Research Goal:

To enable policy makers to make better decisions

View of solution space of the security and usability equation



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) ?

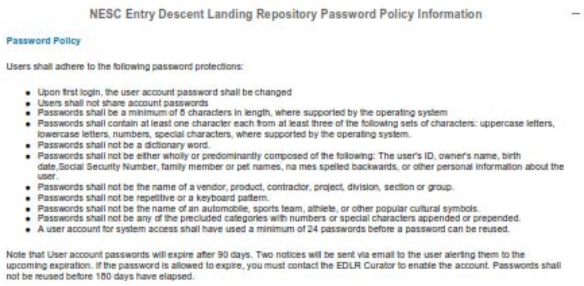
Password specifications as Policies

- 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



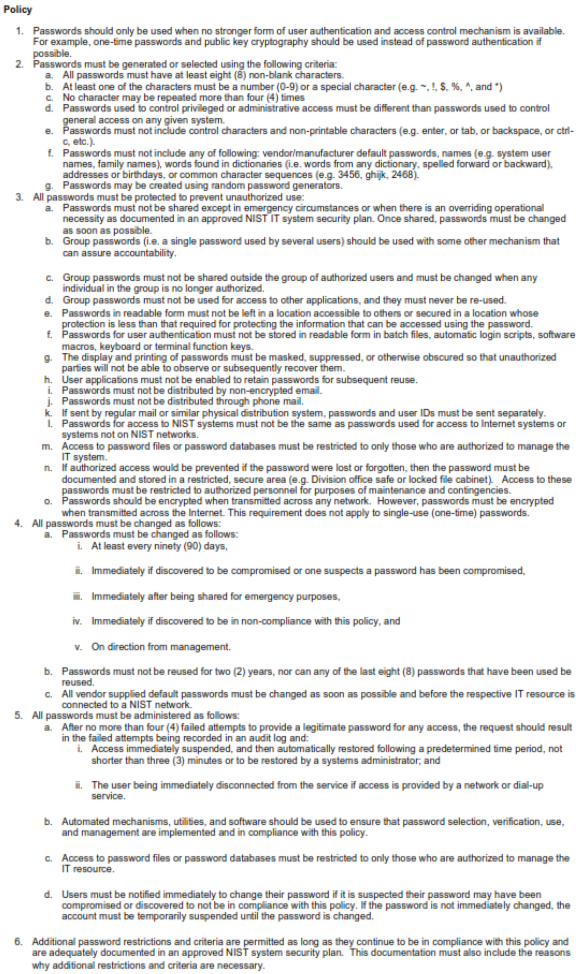
NESC Entry Descent Landing Repository Password Policy Information

Password Policy

Users shall adhere to the following password protections:

- Upon first login, the user account password shall be changed
- Users shall not share account passwords
- Passwords shall be a minimum of 8 characters in length, where supported by the operating system
- Passwords shall contain at least one character each from at least three of the following sets of characters: uppercase letters, lowercase letters, numbers, special characters, where supported by the operating system.
- Passwords shall not be a dictionary word.
- Passwords shall not be either wholly or predominantly composed of the following: The user's ID, owner's name, birth date,Social Security Number, family member or pet names, na mes spelled backwards, or other personal information about the user.
- Passwords shall not be the name of a vendor, product, contractor, project, division, section or group.
- Passwords shall not be repetitive or a keyboard pattern.
- Passwords shall not be the name of an automobile, sports team, athlete, or other popular cultural symbols.
- Passwords shall not be any of the precluded categories with numbers or special characters appended or prepended.
- A user account for system access shall have used a minimum of 24 passwords before a password can be reused.

Note that User account passwords will expire after 90 days. Two notices will be sent via email to the user alerting them to the upcoming expiration. If the password is allowed to expire, you must contact the EDLR Curator to enable the account. Passwords shall not be reused before 180 days have elapsed.



Policy

1. Passwords should only be used when no stronger form of user authentication and access control mechanism is available. For example, one-time passwords and public key cryptography should be used instead of password authentication if possible.
2. Passwords must be generated or selected using the following criteria:
   a. All passwords must have at least eight (8) non-blank characters.
   b. At least one of the characters must be a number (0-9) or a special character (e.g. ~, !, $, %, ^, and *)
   c. No character may be repeated more than four (4) times
   d. Passwords used to control privileged or administrative access must be different than passwords used to control general access on any given system.
   e. Passwords must not include control characters and non-printable characters (e.g. enter, or tab, or backspace, or ctrl-c, etc.).
   f. Passwords must not include any of following: vendor/manufacturer default passwords, names (e.g. system user names, family names), words found in dictionaries (i.e. words from any dictionary, spelled forward or backward), addresses or birthdays, or common character sequences (e.g. 3456, ghijk, 2468).
   g. Passwords may be created using random password generators.
3. All passwords must be protected to prevent unauthorized use:
   a. Passwords must not be shared except in emergency circumstances or when there is an overriding operational necessity as documented in an approved NIST IT system security plan. Once shared, passwords must be changed as soon as possible.
   b. Group passwords (i.e. a single password used by several users) should be used with some other mechanism that can assure accountability.
   c. Group passwords must not be shared outside the group of authorized users and must be changed when any individual in the group is no longer authorized.
   d. Group passwords must not be used for access to other applications, and they must never be re-used.
   e. Passwords in readable form must not be left in a location accessible to others or secured in a location whose protection is less than that required for protecting the information that can be accessed using the password.
   f. Passwords for user authentication must not be stored in readable form in batch files, automatic login scripts, software macros, keyboard or terminal function keys.
   g. The display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.
   h. User applications must not be enabled to retain passwords for subsequent reuse.
   i. Passwords must not be distributed by non-encrypted email.
   j. Passwords must not be distributed through phone mail.
   k. If sent by regular mail or similar physical distribution system, passwords and user IDs must be sent separately.
   l. Passwords for access to NIST systems must not be the same as passwords used for access to Internet systems or systems not on NIST networks.
   m. Access to password files or password databases must be restricted to only those who are authorized to manage the IT system.
   n. If authorized access would be prevented if the password were lost or forgotten, then the password must be documented and stored in a restricted, secure area (e.g. Division office safe or locked file cabinet). Access to these passwords must be restricted to authorized personnel for purposes of maintenance and contingencies.
   o. Passwords should be encrypted when transmitted across any network. However, passwords must be encrypted when transmitted across the Internet. This requirement does not apply to single-use (one-time) passwords.
4. All passwords must be changed as follows:
   a. Passwords must be changed as follows:
      i. At least every ninety (90) days,
      ii. Immediately if discovered to be compromised or one suspects a password has been compromised,
      iii. Immediately after being shared for emergency purposes,
      iv. Immediately if discovered to be in non-compliance with this policy, and
      v. On direction from management.
   b. Passwords must not be reused for two (2) years, nor can any of the last eight (8) passwords that have been used be reused.
   c. All vendor supplied default passwords must be changed as soon as possible and before the respective IT resource is connected to a NIST network.
5. All passwords must be administered as follows:
   a. After no more than four (4) failed attempts to provide a legitimate password for any access, the request should result in the failed attempts being recorded in an audit log and:
      i. Access immediately suspended, and then automatically restored following a predetermined time period, not shorter than three (3) minutes or to be restored by a systems administrator; and
      ii. The user being immediately disconnected from the service if access is provided by a network or dial-up service.
   b. Automated mechanisms, utilities, and software should be used to ensure that password selection, verification, use, and management are implemented and in compliance with this policy.
   c. Access to password files or password databases must be restricted to only those who are authorized to manage the IT resource.
   d. Users must be notified immediately to change their password if it is suspected their password may have been compromised or discovered to not be in compliance with this policy. If the password is not immediately changed, the account must be temporarily suspended until the password is changed.
6. Additional password restrictions and criteria are permitted as long as they continue to be in compliance with this policy and are adequately documented in an approved NIST system security plan. This documentation must also include the reasons why additional restrictions and criteria are necessary.

Goal

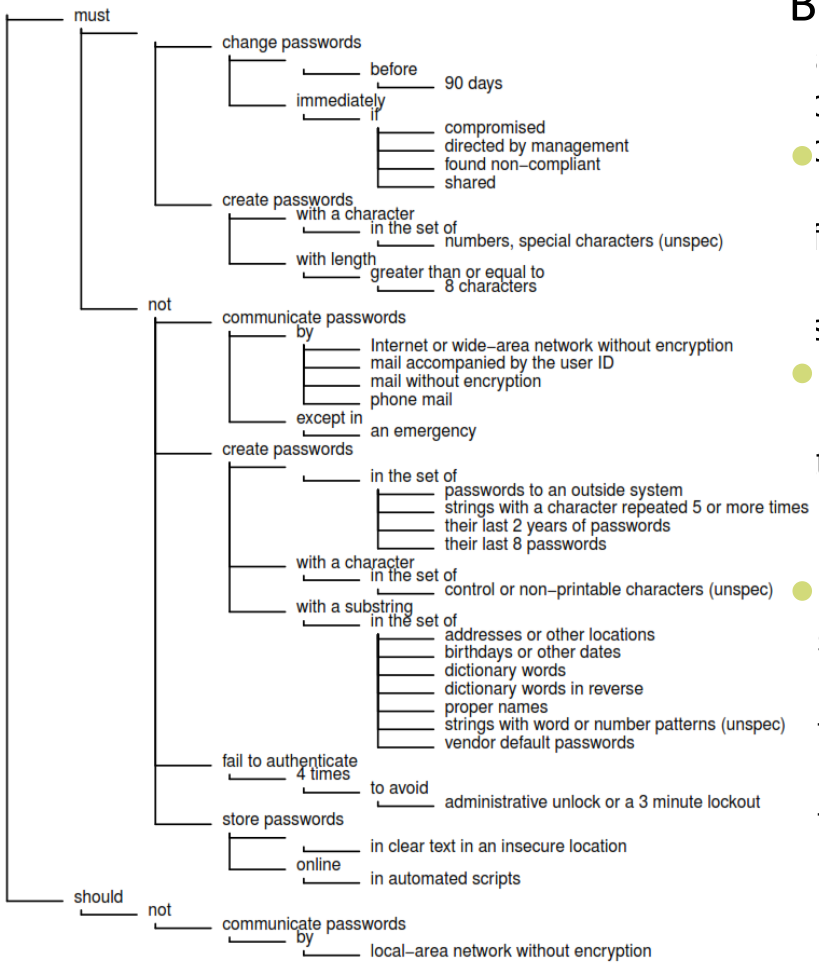
Develop a effective approach for studying password policies.

- 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:

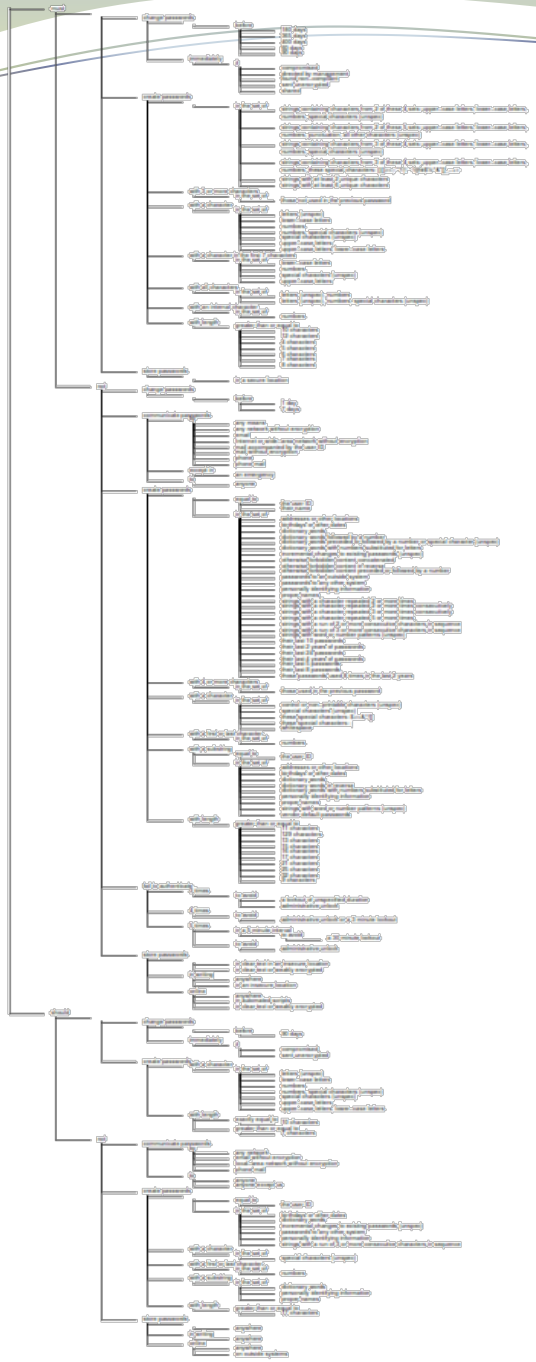


Benefits of a formal (EBNF) grammar:

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

Apply Taxonomy to a Corpus

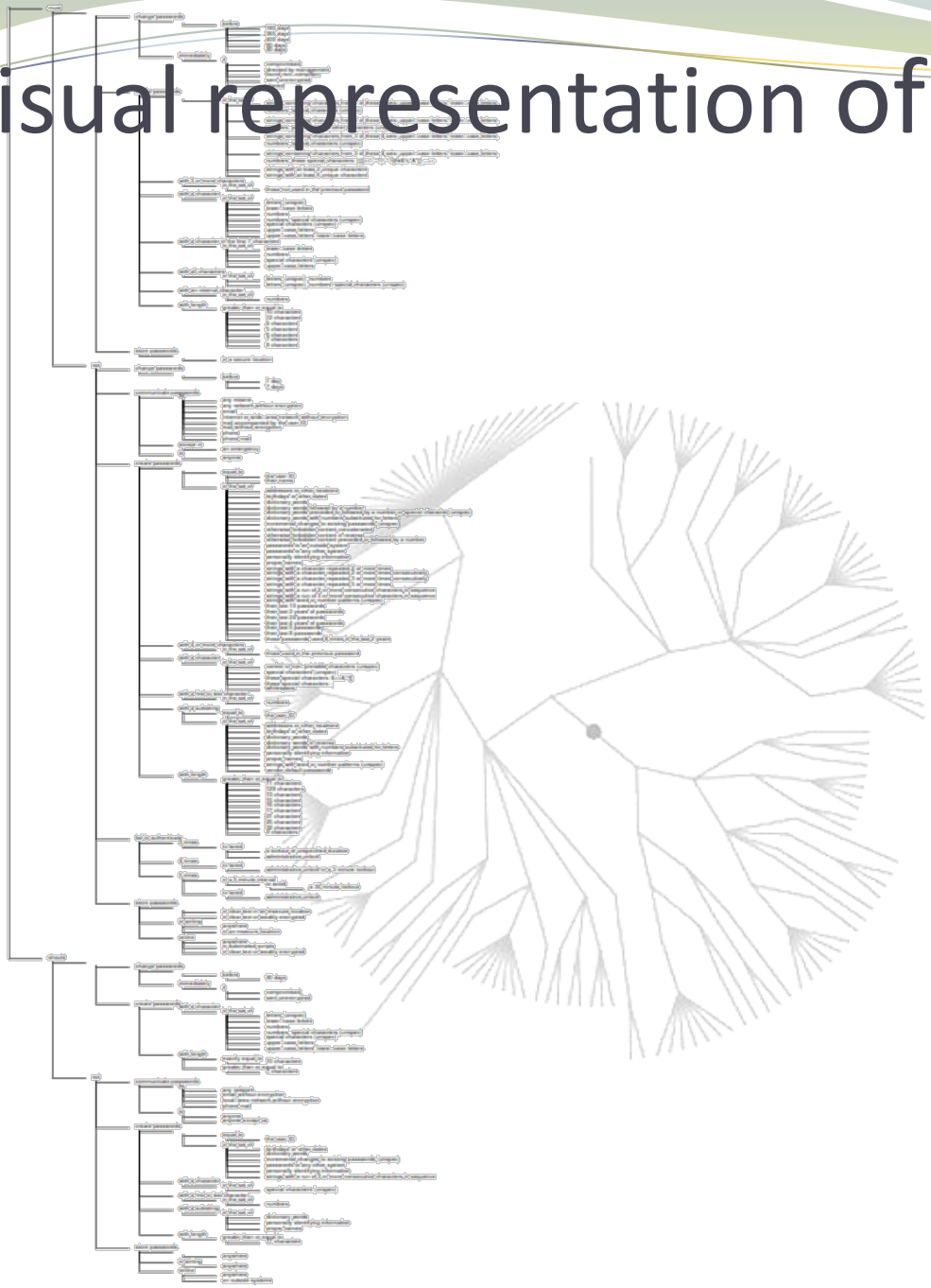
- Corporate and government policies of primary interest (22)
- Password-protected general websites policies included (19)



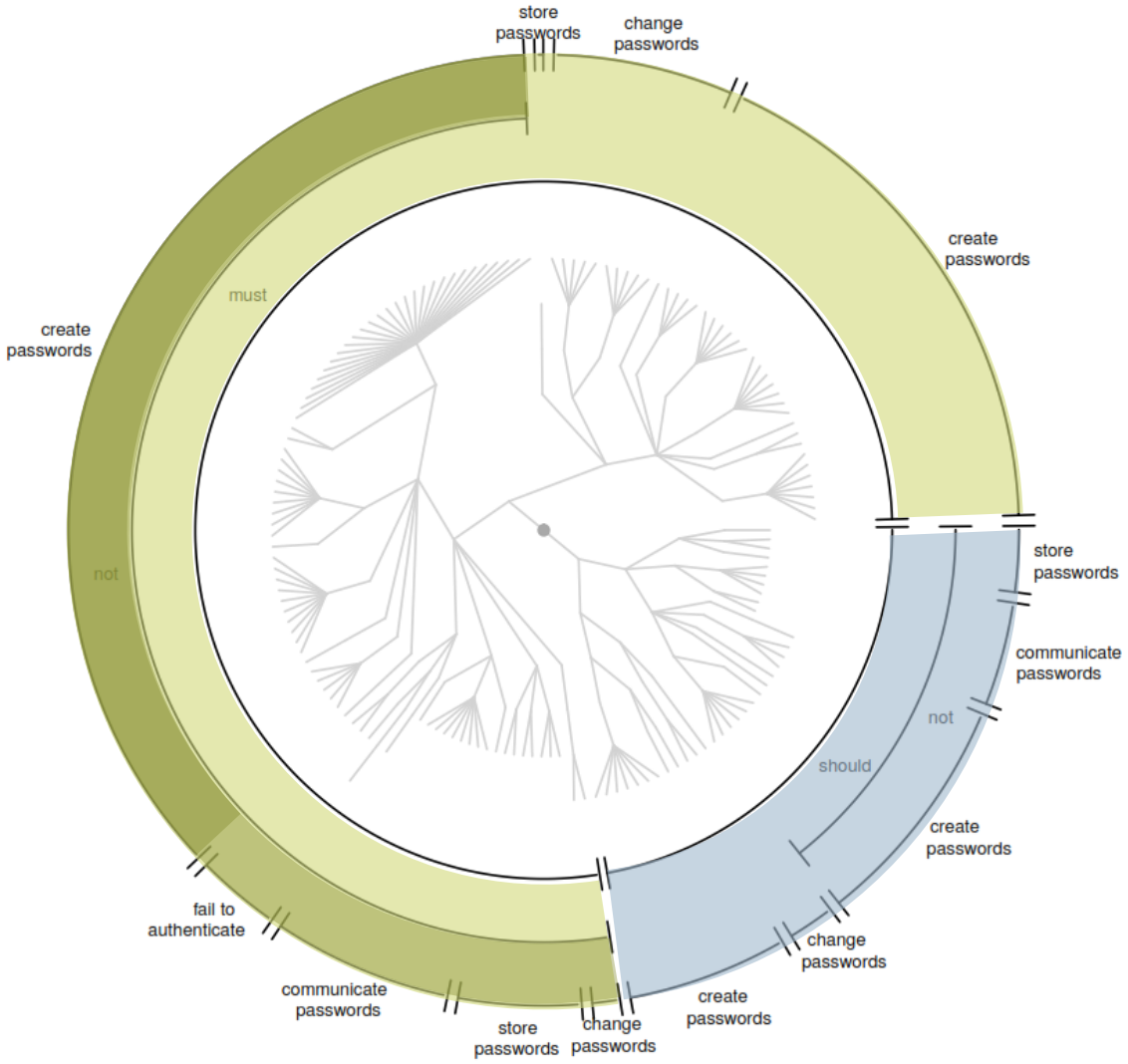
How many different rules?

- 41 policies
- 155 unique rules
- 449 total rules

A visual representation of the corpus

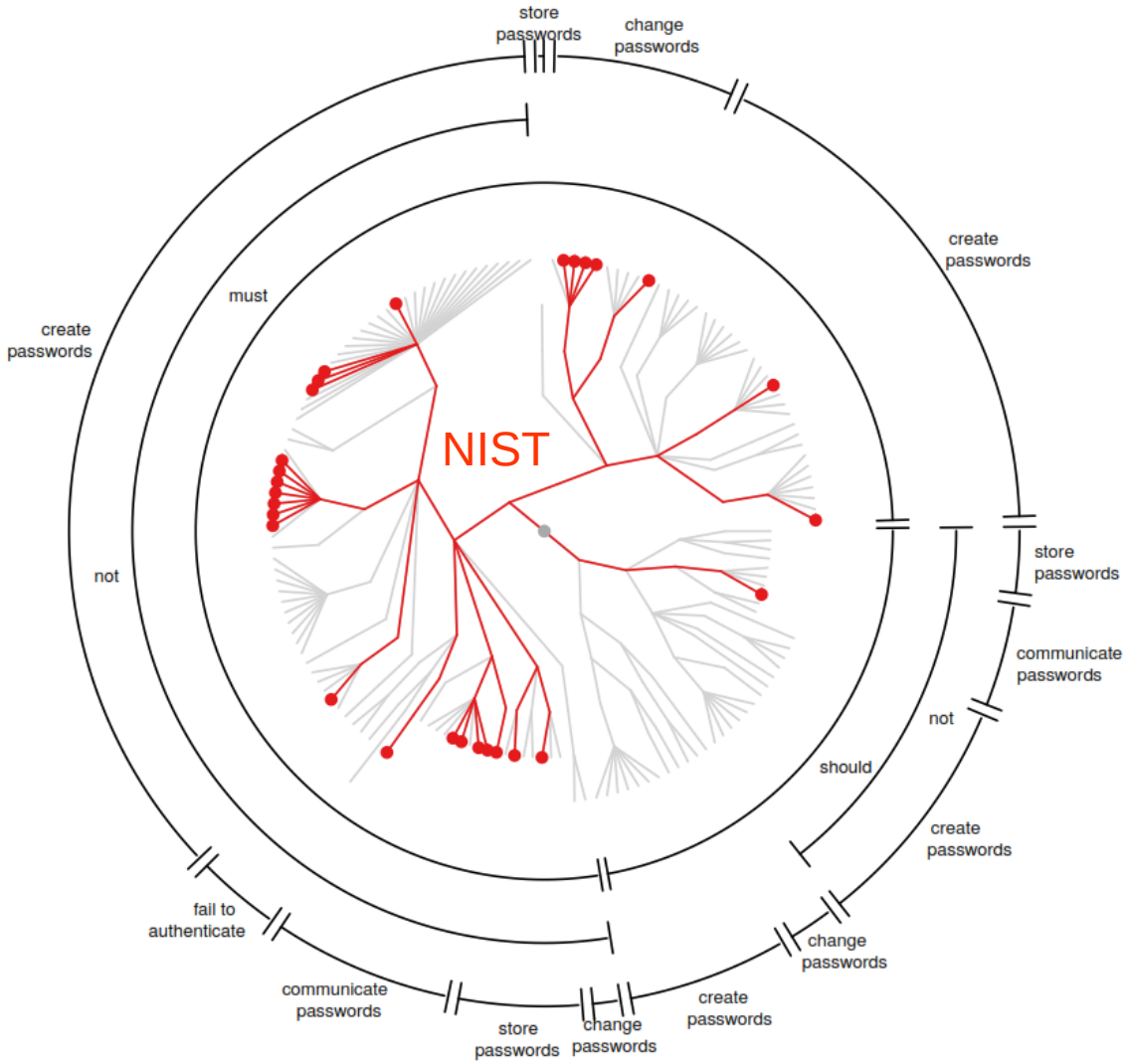


A visual representation of the corpus

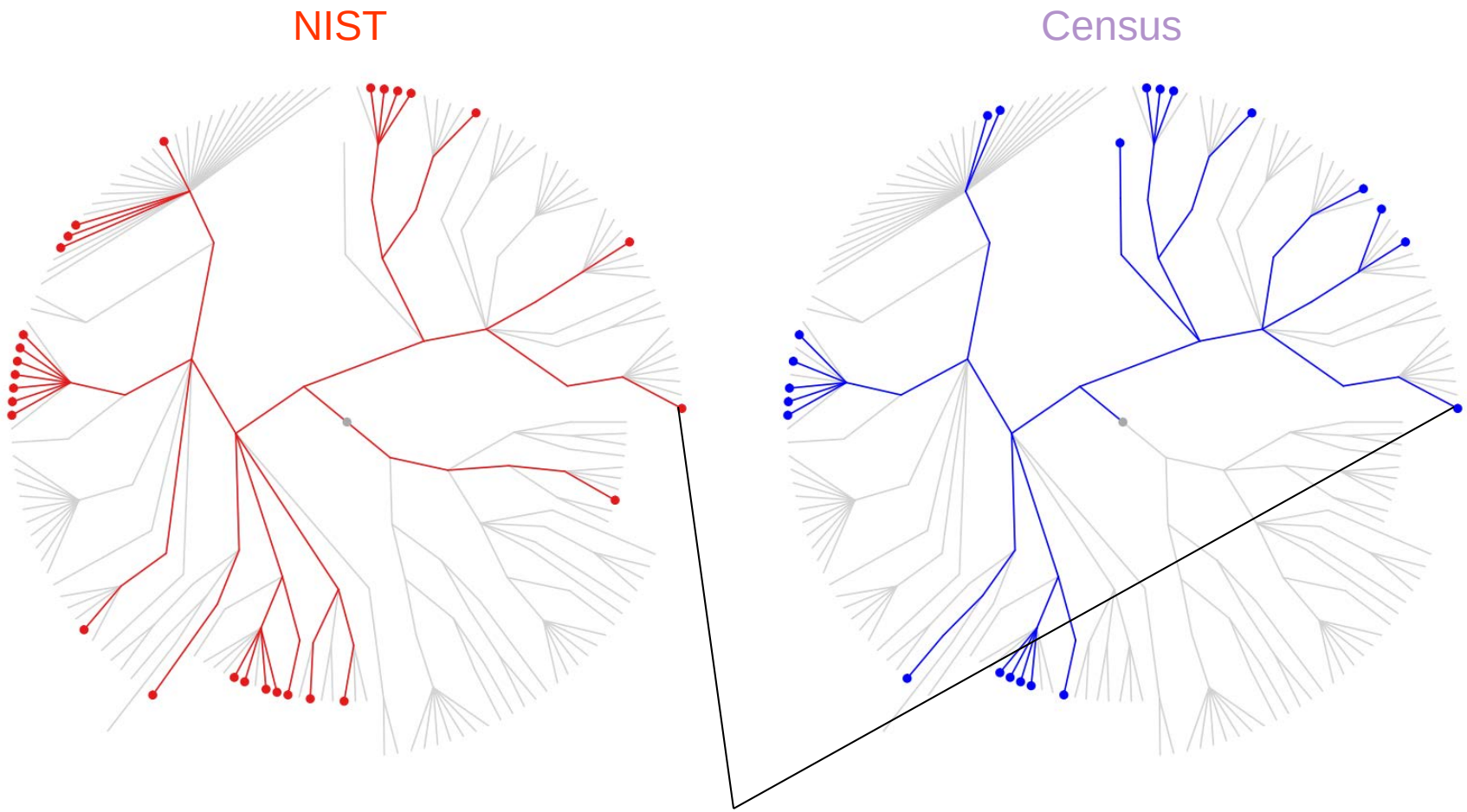


Policy exploration and visualization

Depiction of a password policy

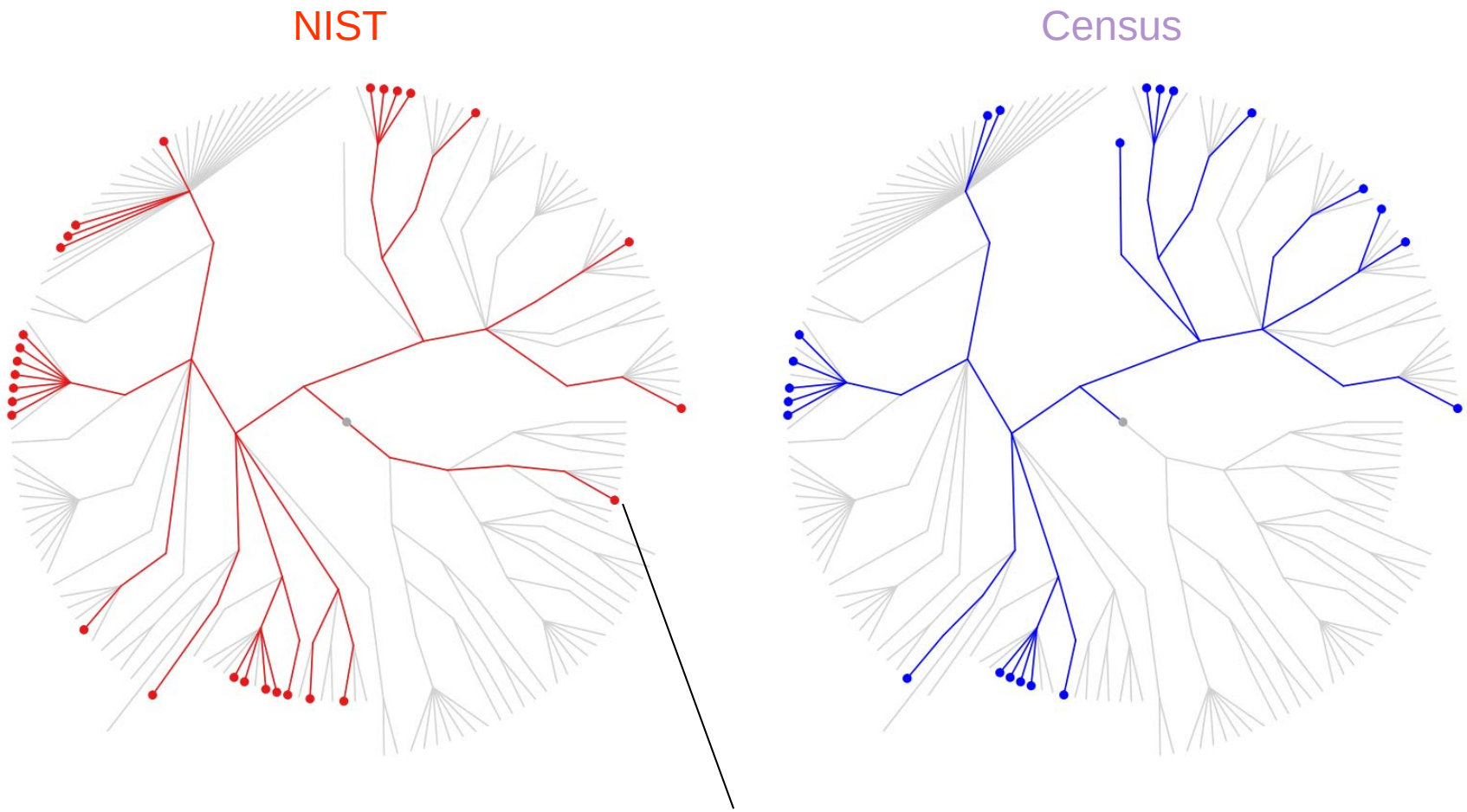


Comparing two policies



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!