Usability Research in Support Of Cyber-Security

Mary Theofanos
Visualization & Usability Group
Information Access Division
Information Technology Laboratory

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

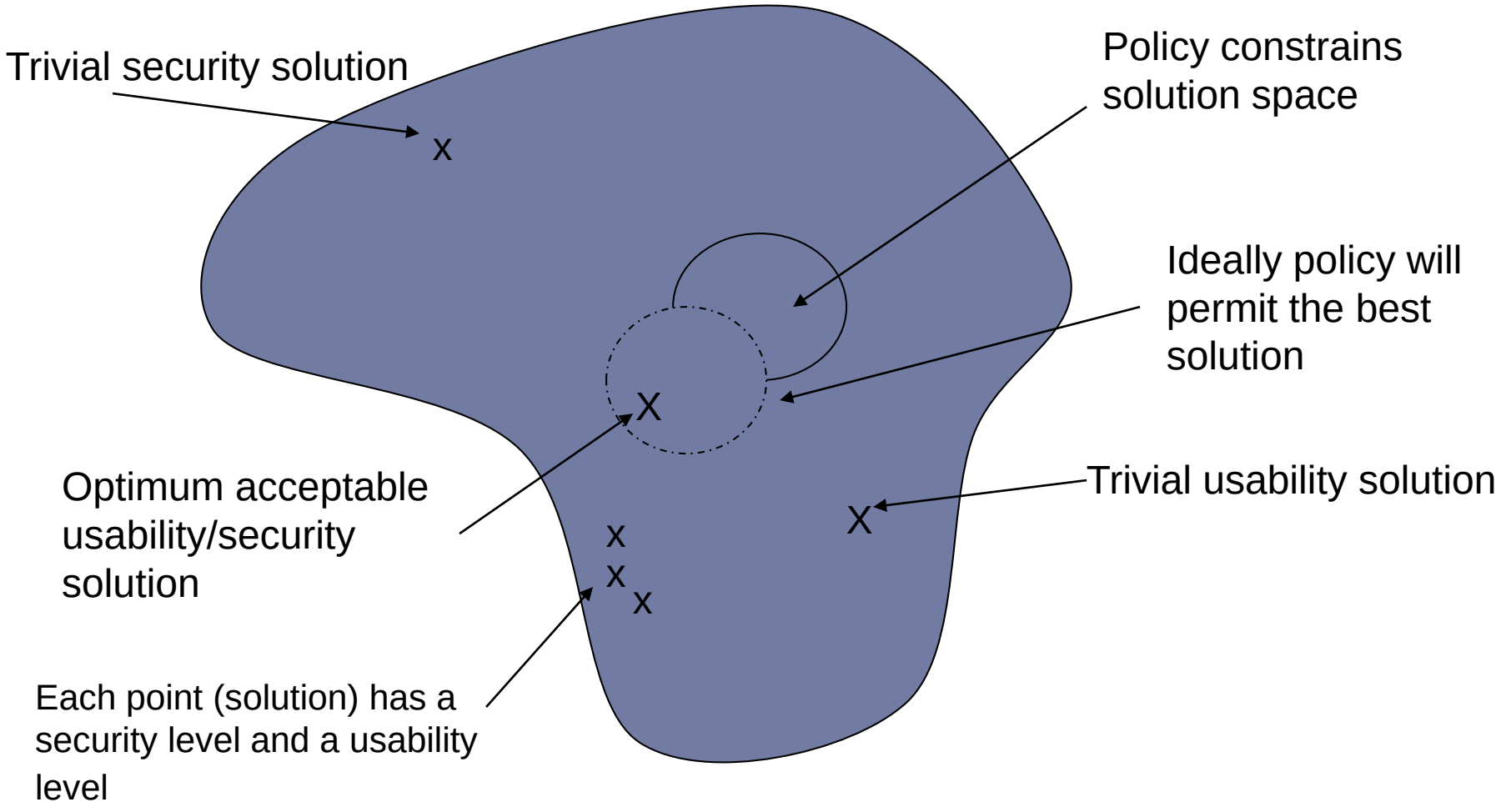
Comprehensive National Cyber-Security Initiative:

- Research and Development

Usability Research Goal:

To enable policy makers to make better decisions

View of solution space of the security and usability equation



Four Primary Research Areas

1. Passwords
2. Password Policies
3. Multi-Factor Authentication
4. Usability and Security Framework

Password Usability Research Goal:

To enable decision makers to make better password policies

- Based on actual data
- Secure in practice not just secure in theory
- Takes into account user behavior

Research requires gathering data

- Instrument is a comprehensive survey of password usage and management
- Survey has been independently reviewed by experts in questionnaire design from Bureau of Labor Statistics
- Responses are anonymous to prevent misuse, but with some demographics
- Survey is for Federal employees only
- Currently being piloted across NIST
- Survey is low impact (estimated 15 minutes)

Password Survey:

It's a matter of perspective

Usability View

- Password creation strategies
- Password management strategies
- Perception of policies/security
- Annoyance Factors

Security View

- Authentication
- Compliance
- Training Needs

Password Survey Questions

Password Survey

- How many passwords do you use?
- Do you use the same password on different accounts?
- How much time does it take to create a password?
- How do you keep track of your passwords?

10. How do you **keep track** of your frequently used passwords? (check all that apply)

- ☐ Do not track, use "forgot password" feature
- ☐ Have someone (e.g., secretary) manage passwords for you
- ☐ Let browser auto-fill
- ☐ Memorize the passwords
- ☐ Rely on hints provided by system
- ☐ Save in a document/file, protected with encryption or password
- ☐ Save in a document/file, not protected (i.e., without encryption or password)
- ☐ Share with a colleague, in case you forget
- ☐ Store in unencrypted electronic devices (e.g., USB flash drive, PDA, cell phone, etc.)
- ☐ Store in agency-managed, encrypted electronic devices (e.g., BlackBerry)
- ☐ Use mnemonics (e.g., meaningful phrase)
- ☐ Use password management software
- ☐ Write down on paper, but disguise in some way (e.g., only write down the common word without the special characters)
- ☐ Write entire password down on paper and store securely in a locked location
- ☐ Write entire password down on paper and place in an un-locked location
- ☐ Other

If "Other" is checked, please describe

11. In your opinion, how **secure** is your **most frequently** used password?

- ○ Not at all secure, i.e., very easy to guess/crack

To date we have:

- Over 550 responses
- Participants are passionate
- Over 95% use user name and password to authenticate
  - Mean number of passwords 12 (range 1 to 210)
  - Try to use same password for different accounts
  - 70% “track on paper” in some form
- Have interference from multiple policies
- Need to make password policy explicit

Potential Impact

- Results could motivate password policies that are less onerous and more effective
- Wide spread participation will strengthen the results

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-down or store passwords online?

Workplace password policies involve much more than length and lifetime.

Policies vary dramatically in length

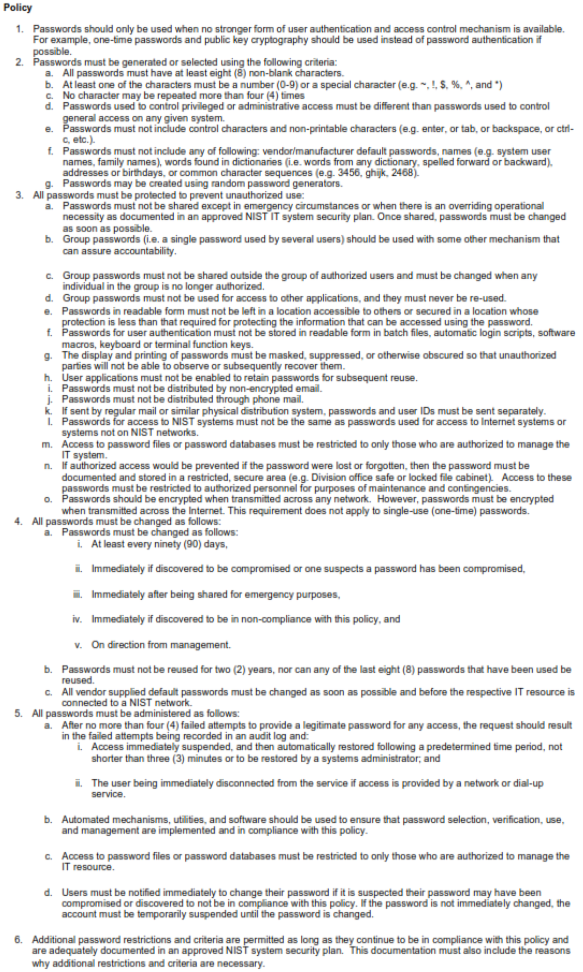
NESC Entry Descent Landing Repository Password Policy Information

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

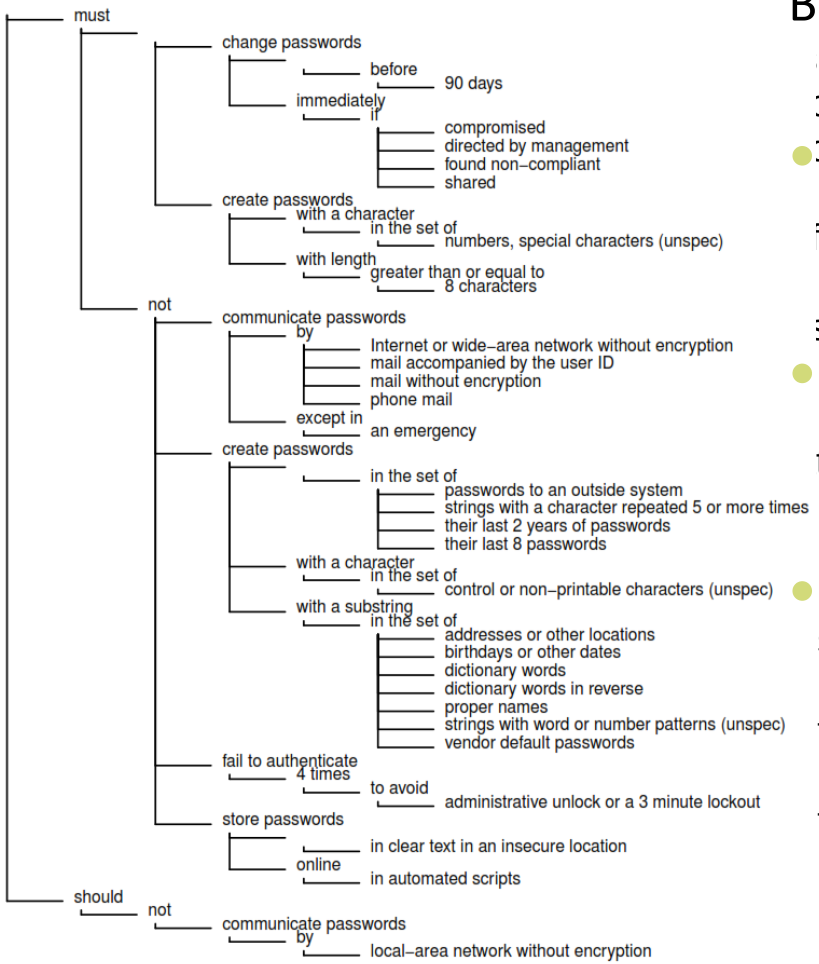
- **Develop a useful password-policy language for studying and improving policies.**

- Specifically, the language should enable us to
  (1) discuss and compare policies, and
  (2) assess how policy rules affect user behavior and security.

- Approach:
  1. **Develop a taxonomy** of policy rules
  2. **Collect a corpus** of representative policies
  3. **Analyze the corpus** using its taxonomic structure

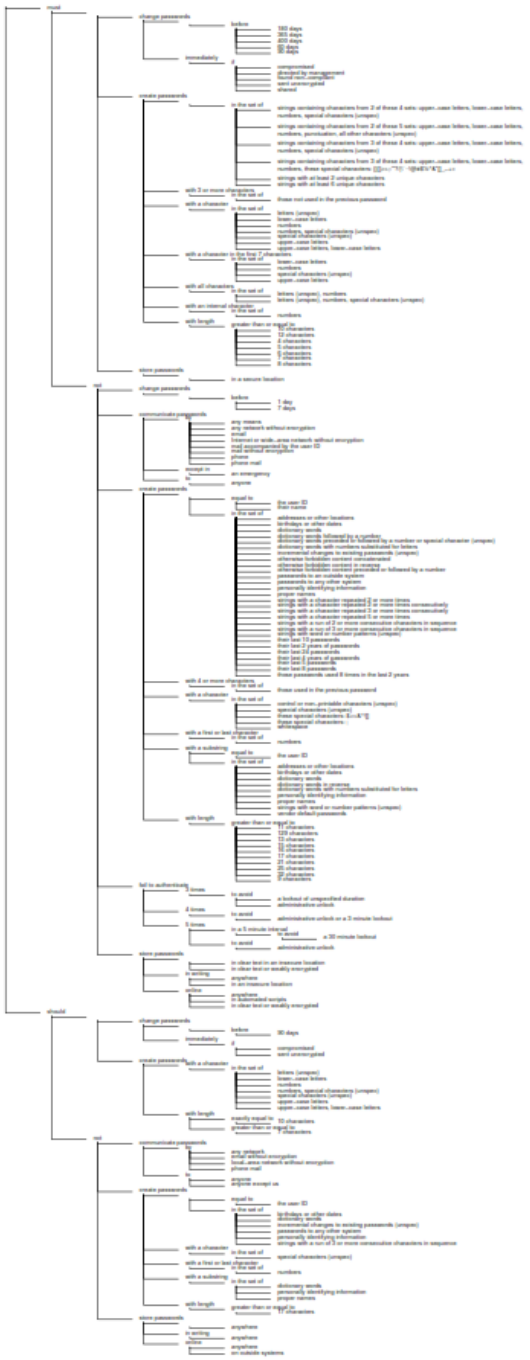
Step 1: Develop a Taxonomy

Reduce policies to an unambiguous language:



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, then other usability issues*)

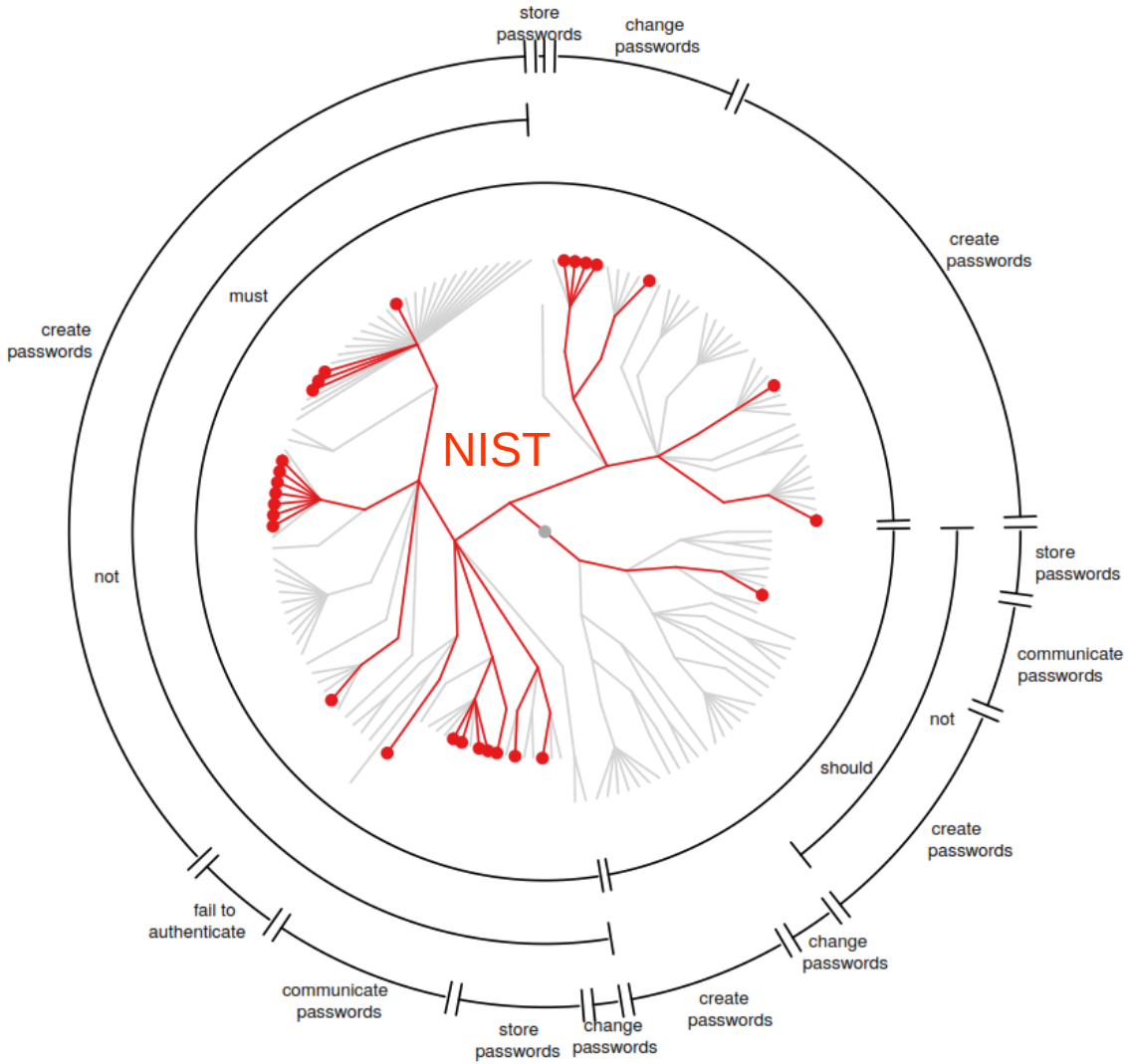


How many different rules?

- 41 policies
- 155 unique rules
- 449 total rules

Policy exploration and visualization

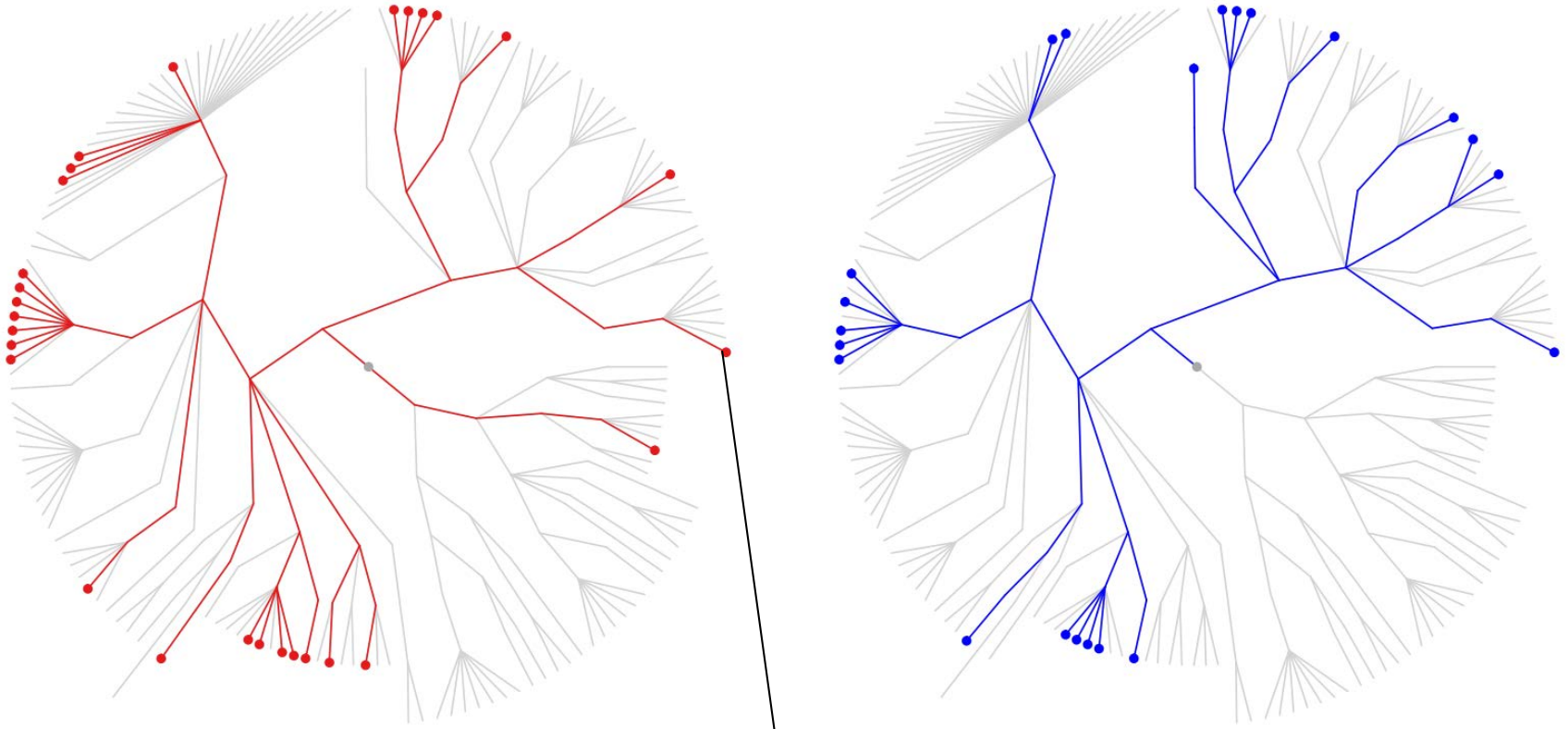
Policy exploration and visualization



Policy exploration and visualization

NIST

Census



Users must create passwords with length greater than or equal to 8 characters.

Basic findings

- A typical policy imposes 10+ rules on a user, and they are not the same from policy to policy.
- The only rule that over half the policies agreed on was an 8-character minimum.
- If users have 3-5 passwords, they **will not** be able to keep all the requirements straight.
- Nearly every policy had ill-formed requirements that make it impossible for a user to comply with certainty.

Potential applications

- Attach security rationale to regions of the space.
  - What threat is this space addressing?
  - How much does it help?
- Attach usability concerns.
  - Does this rule make a reasonable demand on a user's capabilities?
  - Will the rule interfere with others?
- Check for consistency and ambiguity.
  - Are the character sets and forbidden content completely specified?
- Explore and establish best practices more rigorously.
  - Which rules appear frequently? Which are anomalies?
  - Are they frequent within similar organizations?

Final remarks

- **Goal: Develop a useful password-policy language for studying and improving policies.**
  Specifically, the language should enable us to

  (1) discuss and compare policies, and

  (2) assess how policy rules affect user behavior and security.

- How do formal languages help with usability?
  - Establish what the security requirements are.
  - Provide a clear behavioral goal for users.
  - Separate policy requirements from user education.

Multi-factor Authentication

- Which factors encourage adoption and which factors discourage adoption
  - Literature search of relevant fields
  - Establishing a database of publications
  - Annotated bibliography of publications
- Test our hypothesis
  - Currently running a diary study in conjunction with a PIV pilot

PIV study objectives

- Investigate and gain insight on the impact of this new system on worker performance
- Explore attitudes people have about this new two-factor authentication system that may affect uptake.
- Learn whether there are differences in users' expectations and attitudes of systems prior to first use and ongoing use.

Scenarios of use

- Login using card and pin
- Digitally sign email
- Encrypt email
- Access web application to register visitors

Data collection instruments

- Daily emails
- Periodic interviews
- Direct observation
- Pre and post surveys

Users concerns included:

- Forgetting card at home
- Leaving the card in the reader
- Session timeouts due to inactivity even though sitting at desk
- Forgetting to use card to login or unlock and using password instead
- Forgetting password

Ah, they'll get used to it

Framework for Usability and Security

- Recognizes that security is not the primary task
- Recognizes that both disciplines must work together
- Development model
- Evaluation model

What is Usability

ISO 13407:1999

"Usability: The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use."

Definition Identifies How to Proceed:

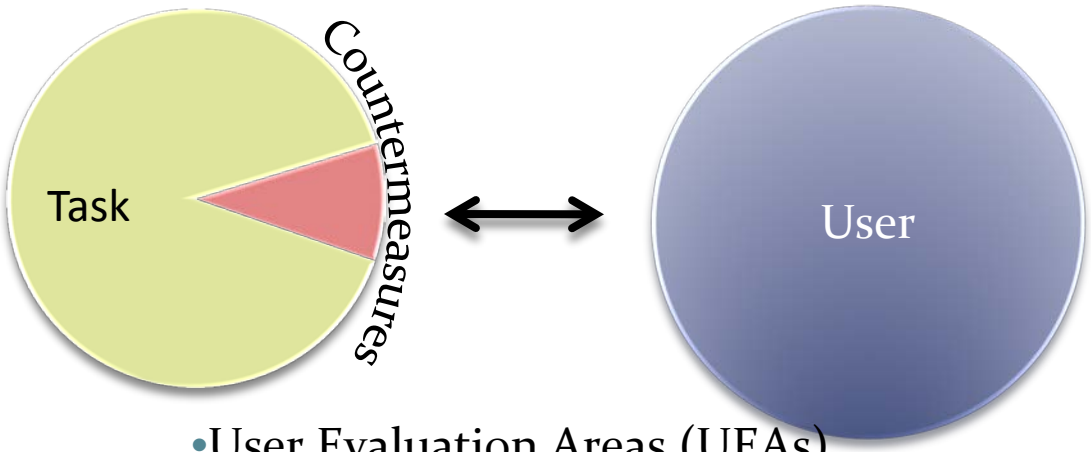
What to measure

- Users
- Goals
- Context of Use

How to measure

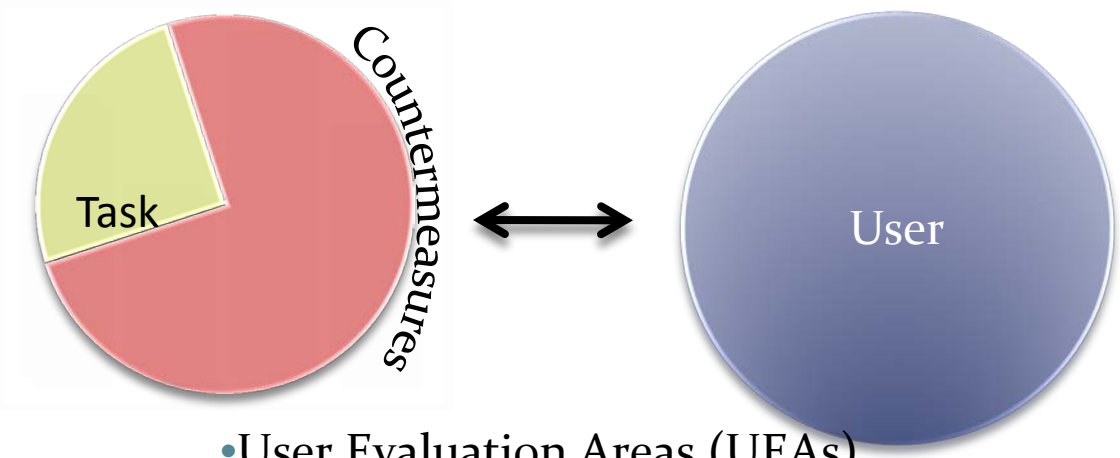
- Effectiveness
- Efficiency
- Satisfaction

Usability



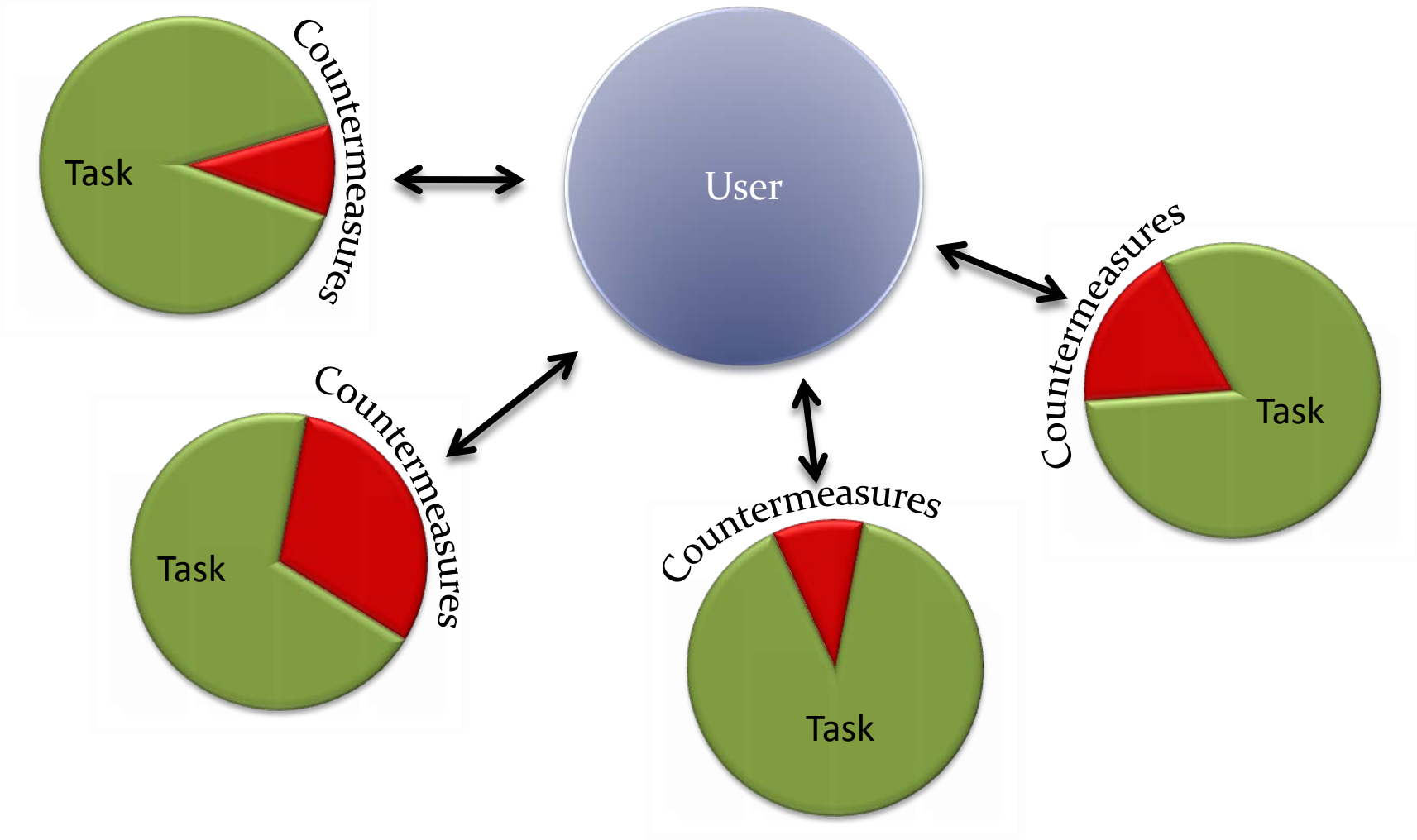
- User Evaluation Areas (UEAs)
  - Attention
  - Adoption
  - Trust
  - Conceptual Models
  - Interaction
  - Invisibility
  - Impact & Side Effects
  - Appeal
  - Application Robustness

Usability and Security



- User Evaluation Areas (UEAs)
  - Attention
  - Adoption
  - Trust
  - Conceptual Models
  - Interaction
  - Invisibility
  - Impact & Side Effects
  - Appeal
  - Application Robustness

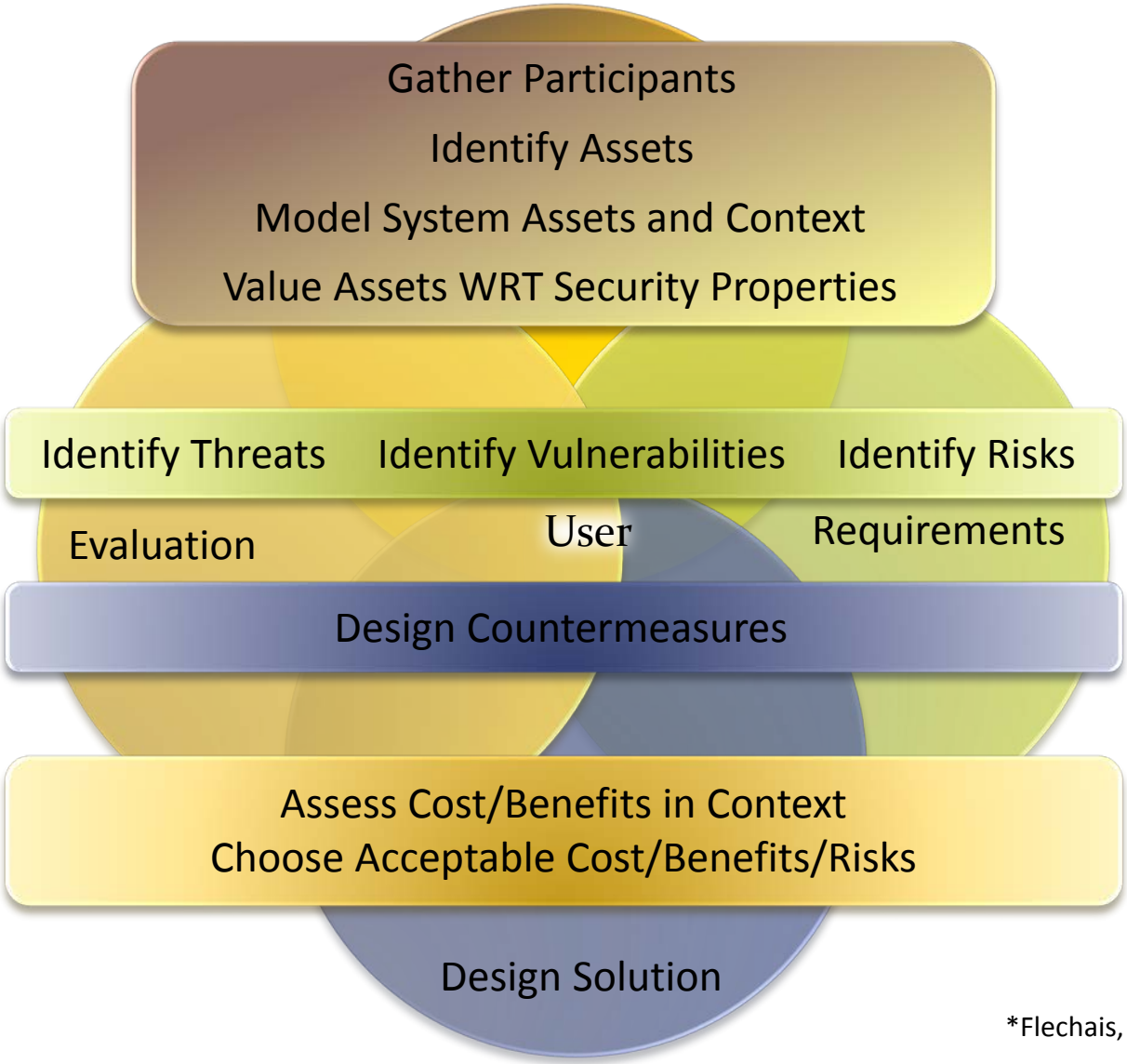
Usability and Security



User Centered Design

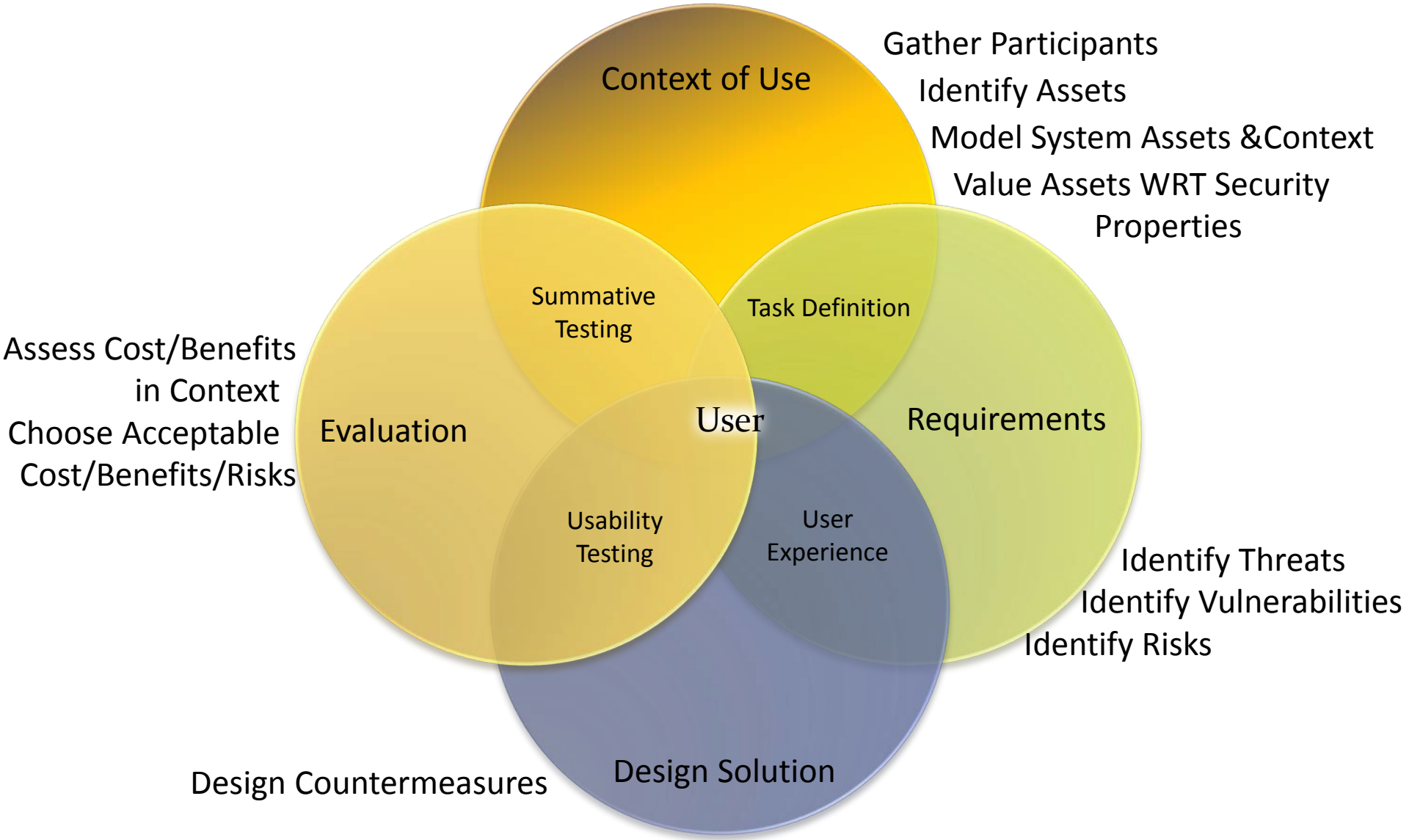
AEGIS Model

Appropriate and **E**ffective **G**uidance for **I**nformation **S**ecurity*

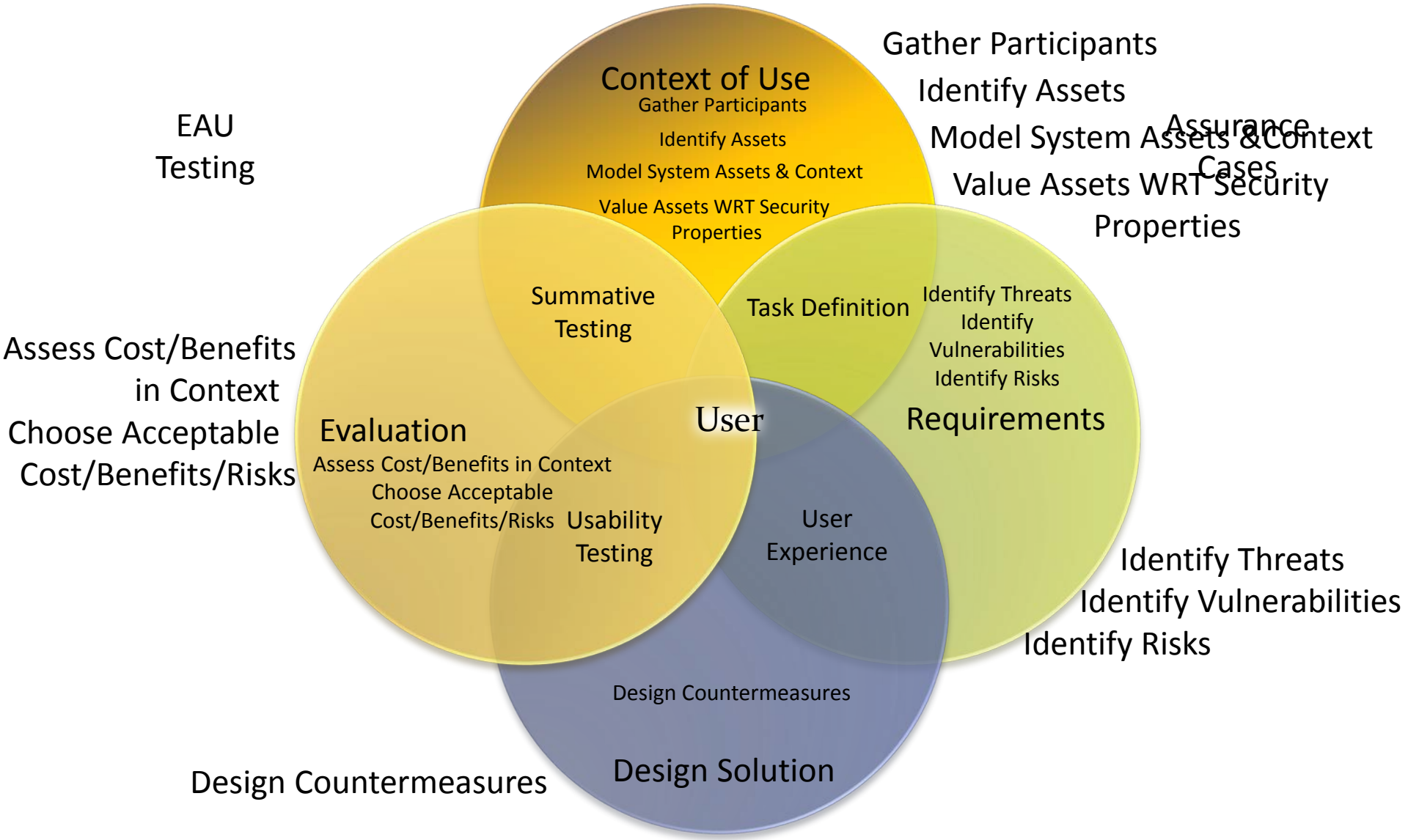


*Flechais, Sasse, & Hailes. 2003

User Centered Design



UCD and AEGIS



Propose : Action-Awareness Framework

1. What is the action that is required to meet the security requirements?
   - Requires security model
2. What are the usability implications of that action?
   - Requires usability model

Users are critical to cyber-security success

- Must understand user behavior
- Need good studies and data to support policies
- Need inter-disciplinary research
- We have the opportunity