Password Usability

Yee-Yin Choong

Cognitive Scientist

Visualization and Usability Group
Information Access Division
Information Technology Laboratory
National Institute of Standards and Technology

October 23, 2015

Usability: ISO 9241-11

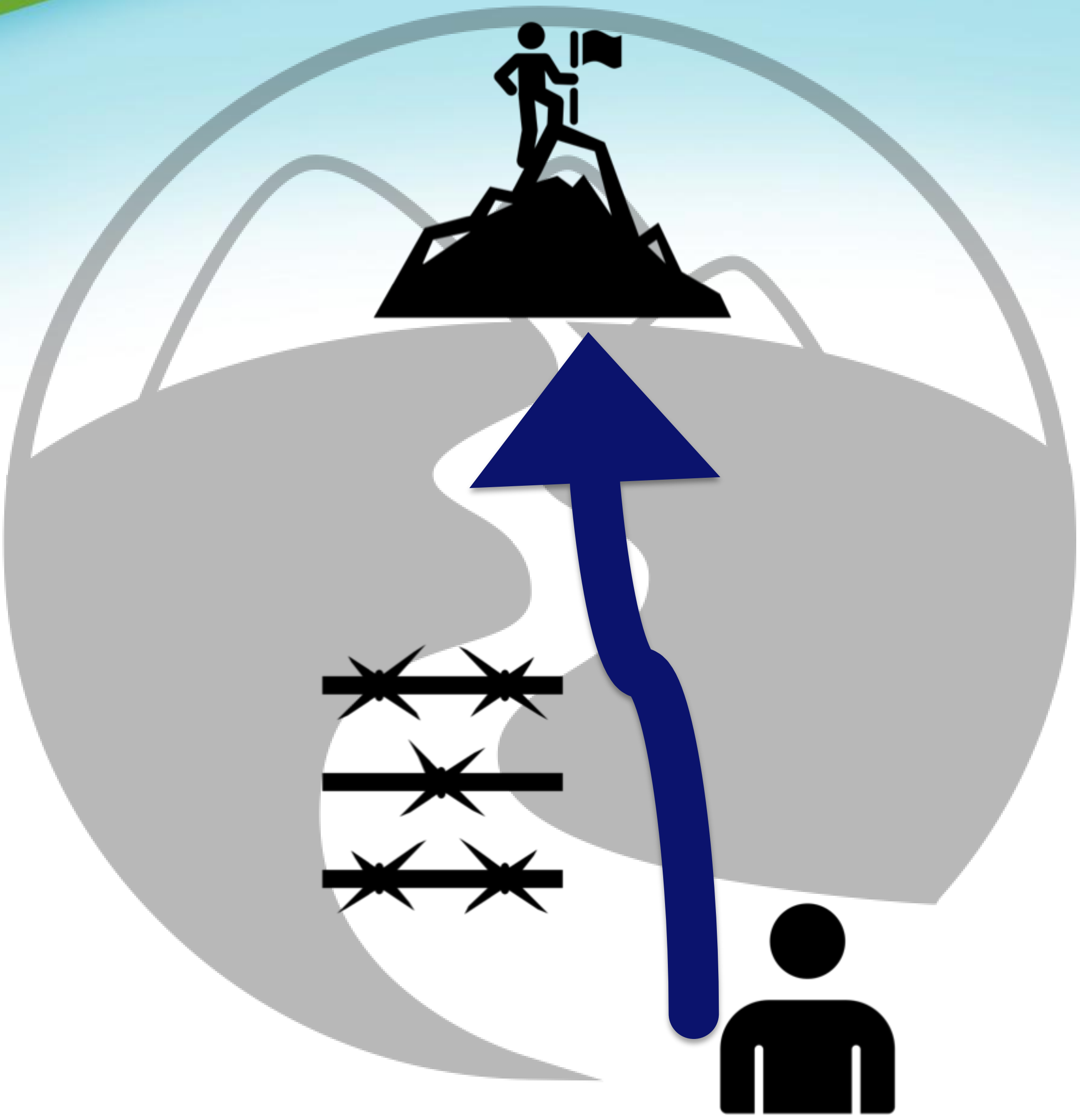
Extent to which a product or system

can be used by **specified users**

to achieve **specified goals**

with *effectiveness*, *efficiency* and *satisfaction*

in a **specified context of use**



Cognitive-Behavioral Framework

Generation

Problem solving

Creative thinking

Decision making

Limited processing capacities

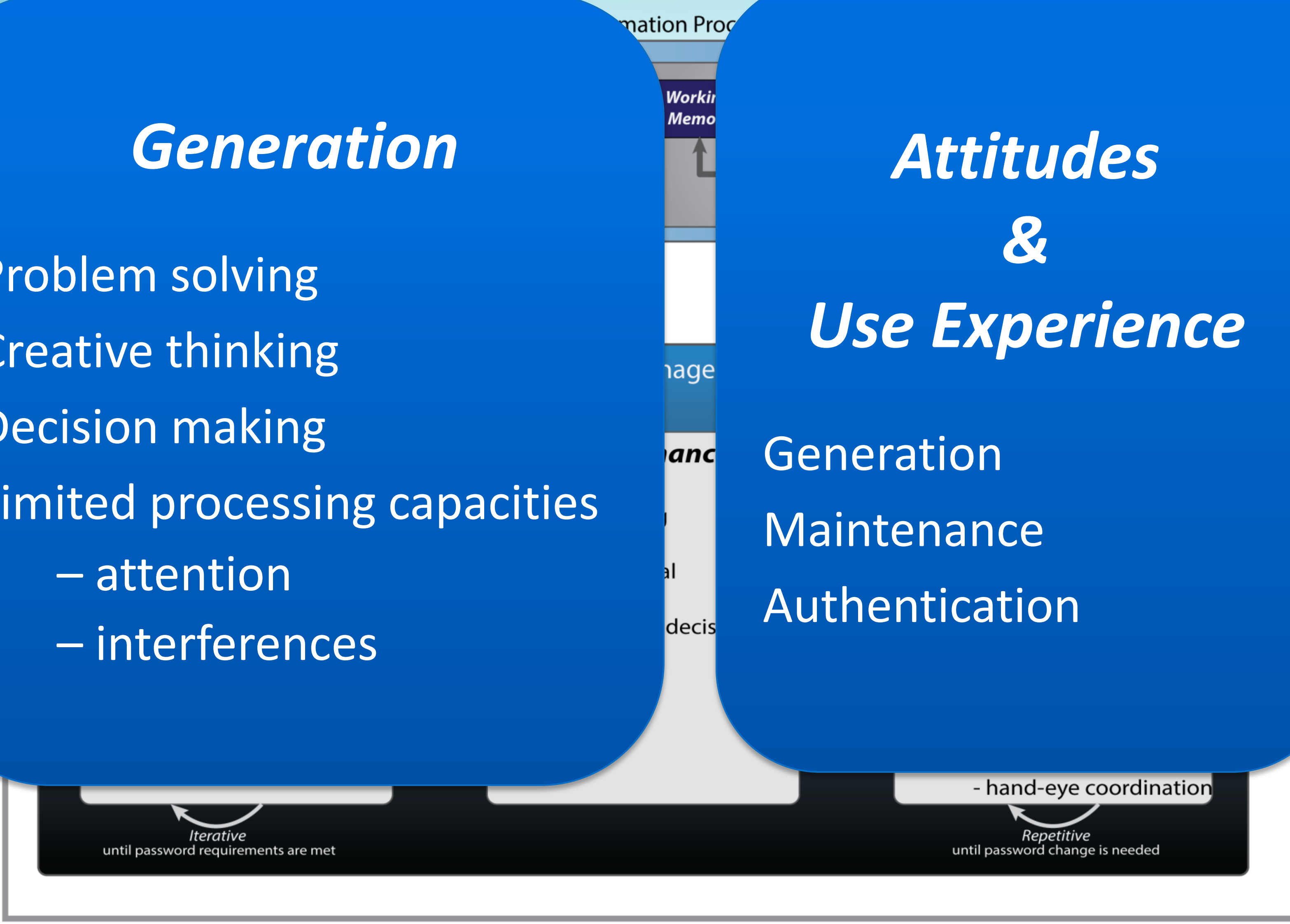
- attention
- interferences

Attitudes & Use Experience

Generation

Maintenance

Authentication



Change password (e.g. forgotten, expiration, compromise, synchronizing with other passwords)

Study 1 – Password Generation Study

- Investigate user password generation space
- Effects of rule presentation formatting
- Participants
  - 81 participants
  - Average age: 35.1 (years)
  - 53% female, 47% male

Experimental Design

- Two sets of password rules (within-Subject)
  - Complex
  - Simple
- Two presentation styles (between-Subject)
  - Formatted
  - Unformatted
- **Data**
  - Number of passwords generated
  - Password generation time
  - Time to 1st Keypress and Password
  - Character Type Distribution
  - Character Type Positioning

Presentation Style	Password Rules	
	Complex	Simple
Formatted n=40	Your password **must have**: • at least 12 characters • at least 1 uppercase letter (A to Z) • at least 1 lowercase letter (a to z) • at least 1 number (0 to 9) • at least 1 symbol. Your password **must not**: • have 5 occurrences of the same characters • Contain any dictionary words.	Your password **must have**: • at least 6 characters. You can use **any characters** that can be typed on a standard keyboard. Password tip: It is recommended that you use a combination of upper and lower case letters, numbers and symbols.
Unformatted n=41	Your password must be a minimum of twelve characters in length. Each password must contain at least one of each of the following types of characters: uppercase alphabetic (A to Z), lowercase alphabetic (a to z), numeric (0 to 9), and symbols. Your passwords cannot contain any dictionary words. Your passwords cannot have five occurrences of the same character.	You need to create a password of minimum 6 characters long. You can use any characters that can be typed on a standard keyboard. Password tip: It is recommended that you use a combination of upper and lower case letters, numbers and symbols.

Results

- 8,165 passwords generated (81 participants)
  - Complex rules: 3,138 passwords
  - Simple rules: 5,027 passwords
  - Average: 100.8 passwords per participant
- Avg. Time to 1st Keypress
  - Simple = 14.35 s, Complex = 23.98 s
- Avg. Time to 1st Compliant Password
  - Simple = 22.28 s, Complex = 82.65 s

Effects of Presentation Formatting

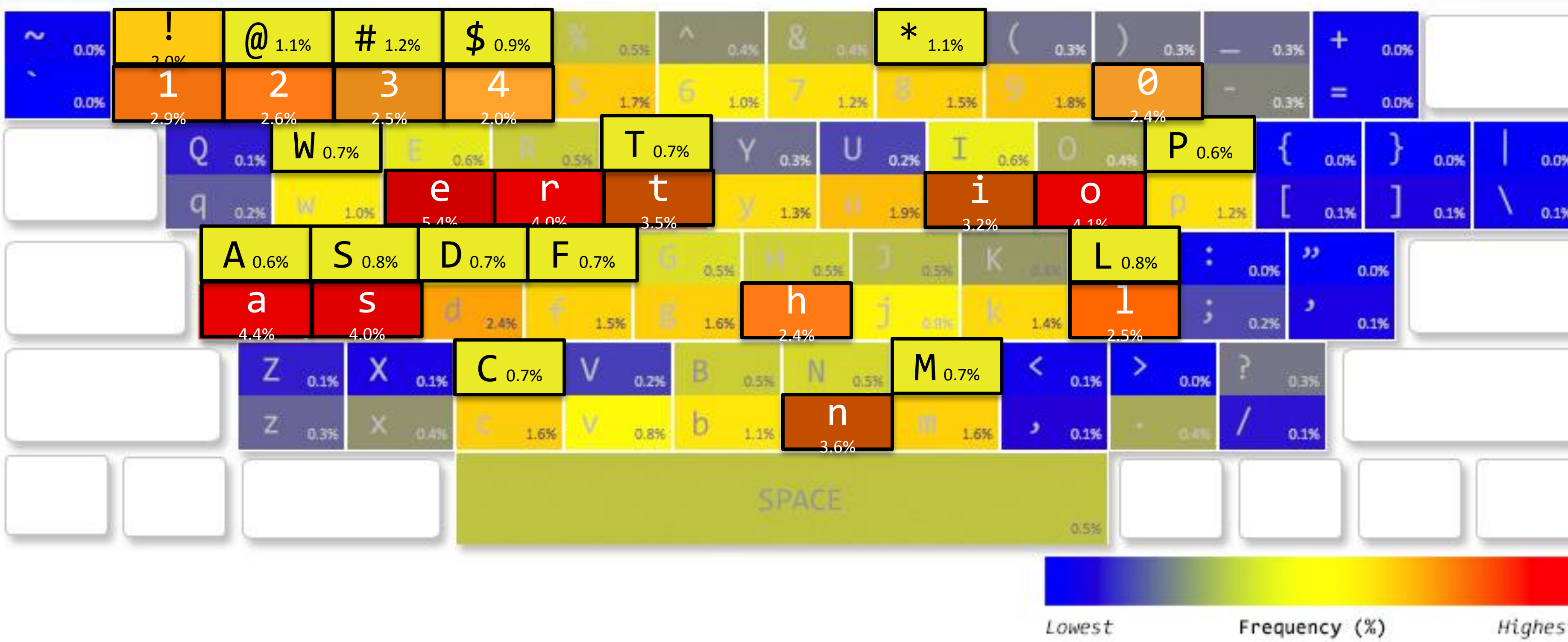
- Formatted Presentation = Better Performance
  - Complex Rules – faster start time

	Formatted	Unformatted
Time to 1st key press	21.2 s	26.7 s
Time to 1st compliant password	79.8 s	85.5 s

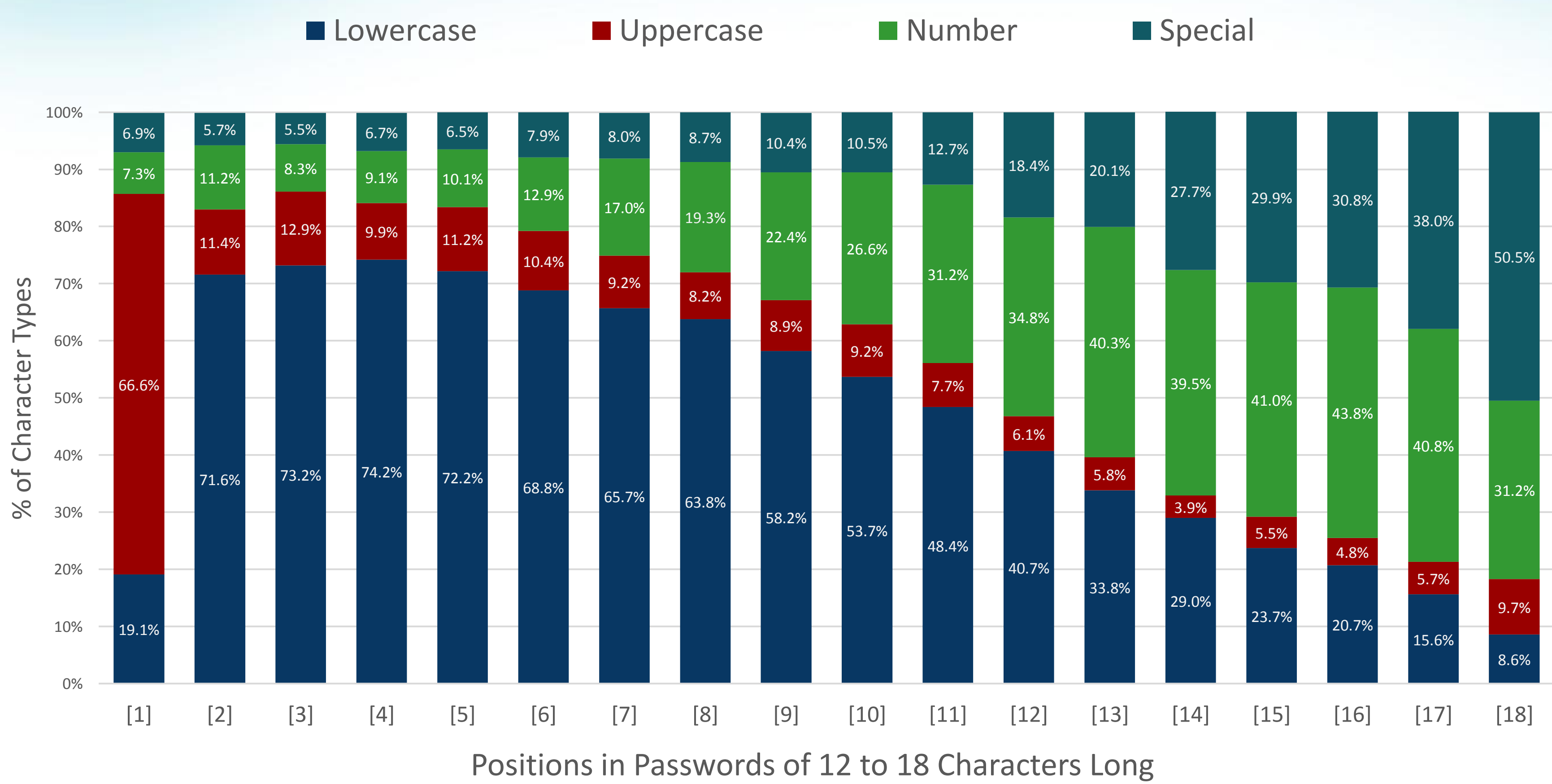
  - Simple Rules – more passwords, shorter time

	Formatted	Unformatted
Number of passwords	69.4	54.9
Password generation time	9.7 s	13.4 s

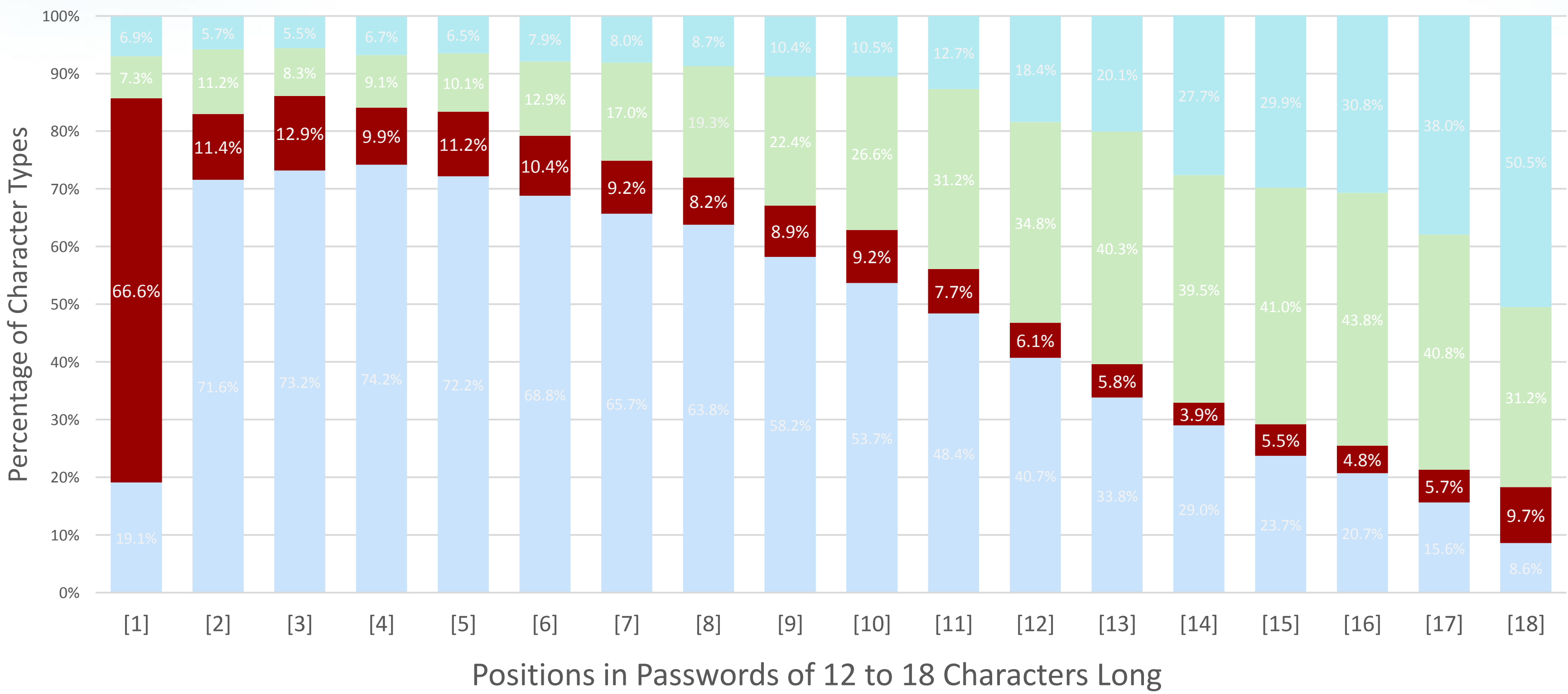
Complex Passwords Heat map



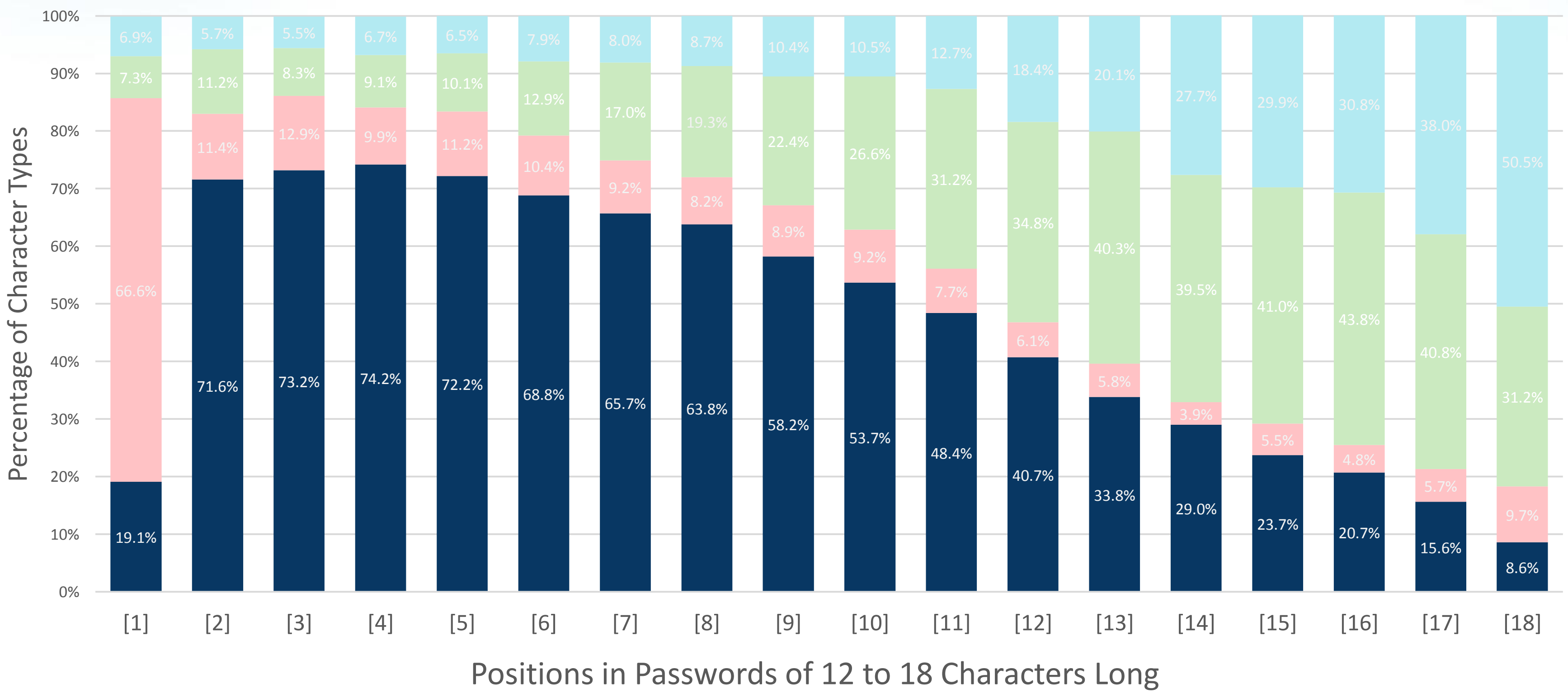
Positioning Patterns



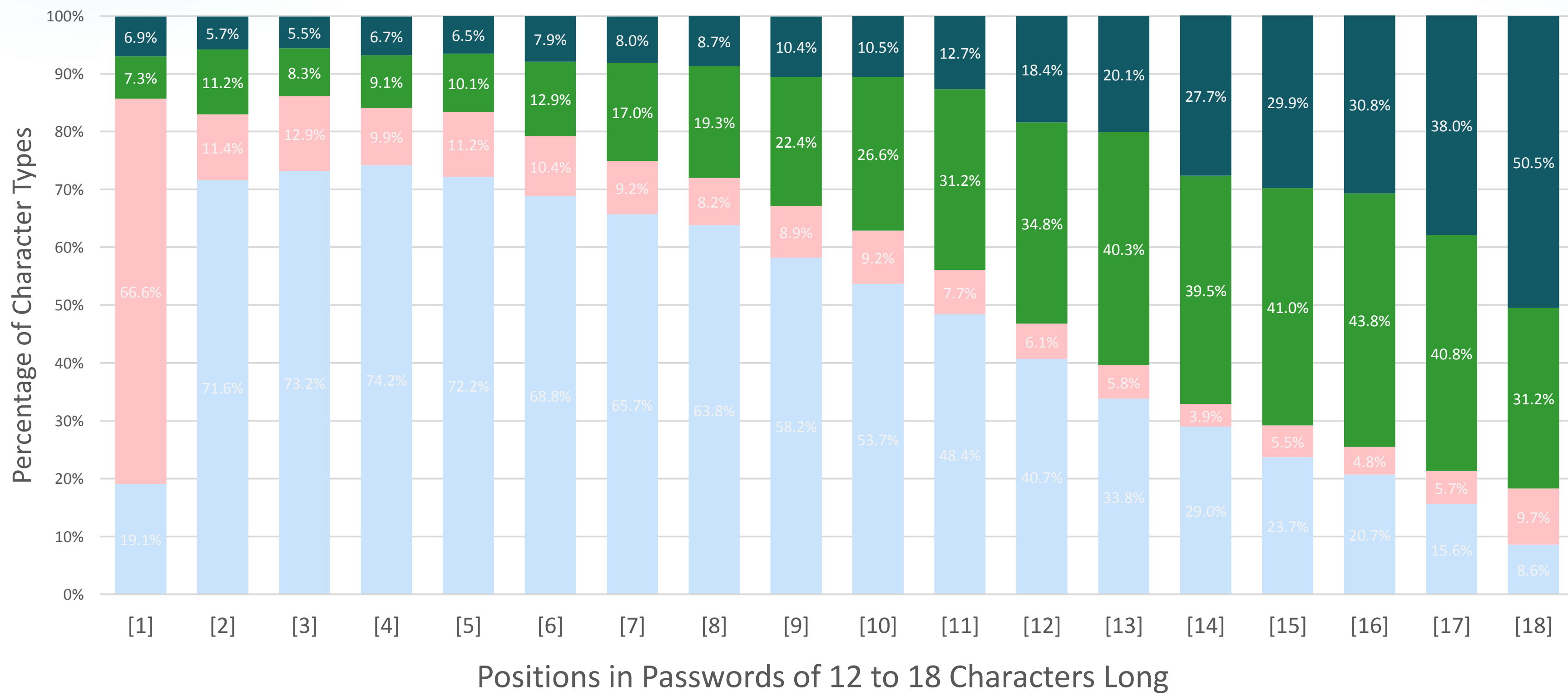
Positioning Patterns – Uppercase



Positioning Patterns – Lowercase



Positioning Patterns – numbers & special characters



Study 2 – Employee Password Usability Survey

- Online Survey (2010-2011)
  - Anonymous
  - Questions on password management and computer security
  - Demographics
- US Government Workers
  - 4,573 Department of Commerce (DOC) employees

Password Usage

- **Average 9 work-related passwords**
  - 5 frequently used
  - 4 occasionally used

- **Time spent on creating passwords**

Password Types	**Estimated Longest Time Total**[1] (Mean)	**Worst Scenario - time spent annually**[2] (with longest time)	
		Hours/employee/year If on a 90-day cycle	Hours/employee/year If on a 60-day cycle
Frequent passwords	98.5 min	6.6 h	9.9 h
Occasional passwords	86.6 min	5.8 h	8.7 h
	Total	**12.4 h**	**18.6 h**

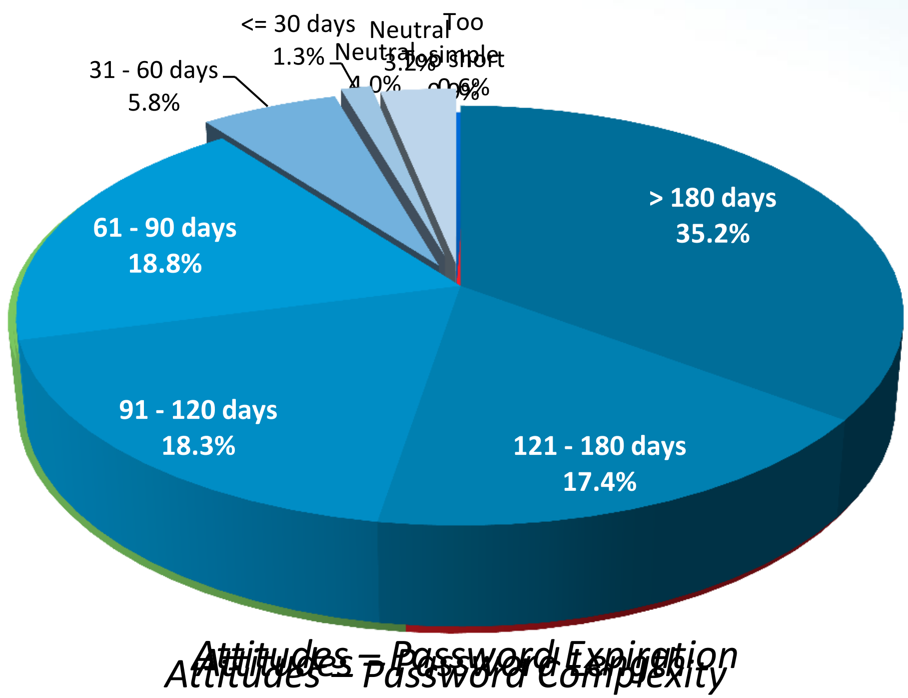
[1] Estimated Longest Time Total = (number of password counts) x (estimated longest time for a password)
[2] The calculation is based on the password changing cycle of 90 days (i.e. 4 times a year), and 60 days (i.e. 6 times a year).

Password creation takes long, why?

- *The program kept rejecting my password because it was not within the guildlines [sic] even though I thought I was following them.*
- *That 25 minutes was actual time trying to get a system to accept a password. I was so desparate [sic] I actually started asking colleagues for suggestions! .*
- *Longer if I manage to lock myself out in doing so, or can't remember what I just changed it to and have to get it reset all over.*
- *sometimes it's taken me 20min to change a password to one that meets the requirements and isn't too far off from my other ones (so I can remember it!)*
- *Longest time is 2 days. The password expired and a default password was set. I could not change away from the default due to a lock out feature requiring that the password not be changed more than once in two days.*
- *There have been several times where it took so long to create a complex enough password that I forgot the password when logging in the next time and had to have it reset.*

Attitudes toward Password Policy

- Too long
- Too complex
- Changed too often
  - not at the same time!



What did they say?

- *The combination of length/complexity, number of different passwords, plus frequent changes makes passwords insecure, because they must be written down.*
- *How do you think people remember extremely complex passwords which also require to be changed every 3 months ? #Wr1T31Td0wN .. yes that's 12 chars :)*
- *I understand that for ""security" " reasons it is good to change a password - but seriously are we all expected to magically remember 12 different passwords, most of which are 10 charecters [sic] long, and can't look like a word (I agree with the reason for the complexity - it just hard on the user).*
- *I make a list of the password requirements for all accounts and make one that fits all of them.*
- *Security has become so complex, it's interfering with being able to do a job efficiently.*
- *It is hard enough to come up with a 12 or so string of unique characters every three months, let alone remember 10 individual ones.*
- *Security has become so complex, it's interfering with being able to do a job efficiently.*

Organizational Password Policy

- Protect data integrity and system security
- Control employees’ access
- Dictate employees’ password management
  - Password composition requirements
  - Password expiration
  - Reuse and history
  - Storage requirements

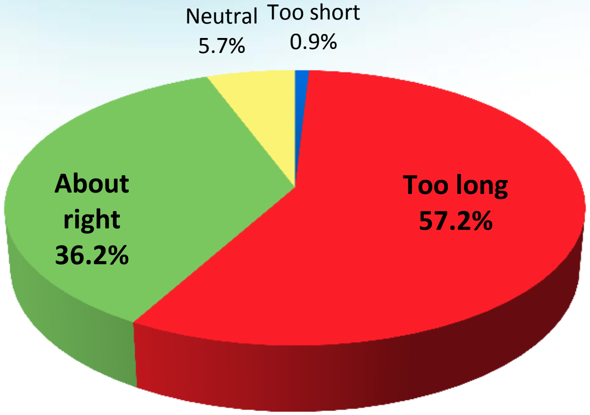
Employee Attitudes

- Attitudes (Fishbein & Ajzen, 1975)

  *"**Learned**, relatively enduring dispositions to respond in consistently favorable or unfavorable ways to certain people, groups, ideas, or situations."*

- Positive employee attitudes
  - combat negative reactions to organization-wide changes or policy viewed as unfavorable

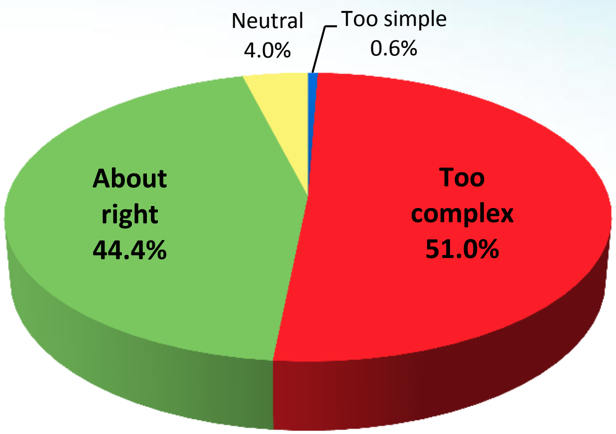
Divergent Views



Attitudes – Password Length

About Right

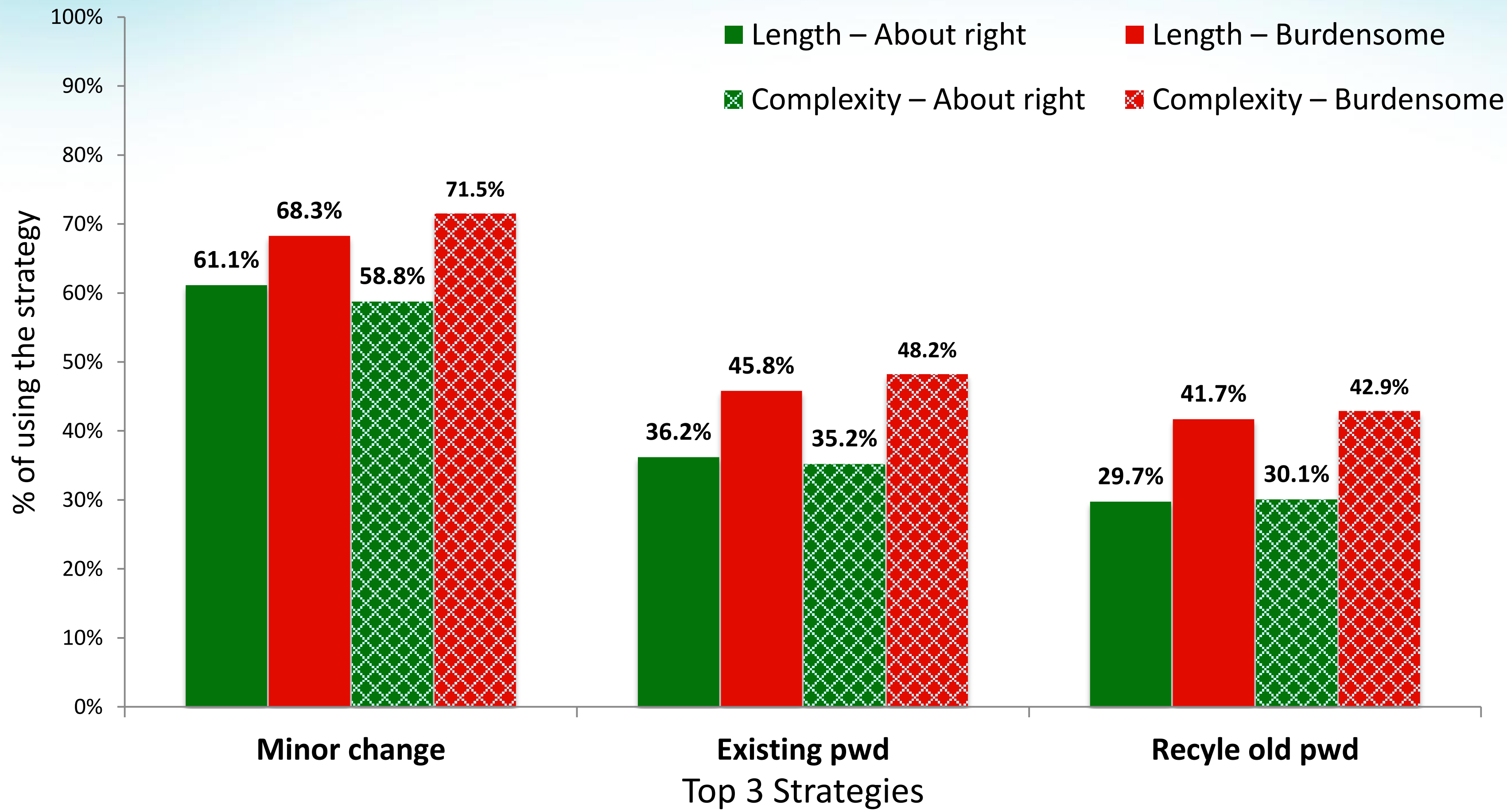
Burdensome



Attitudes – Password Complexity

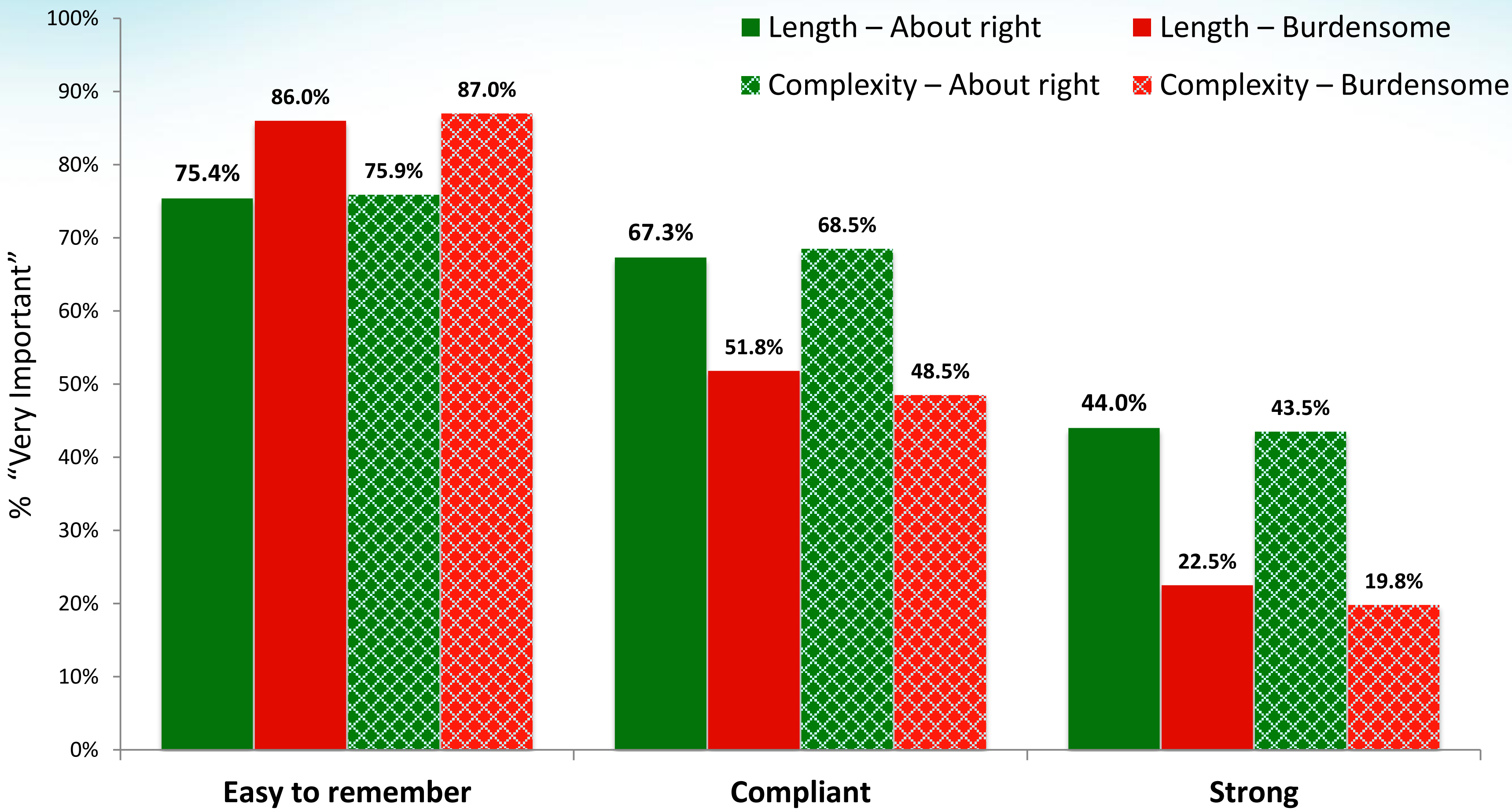
Employee Password Management Lifecycle

Password Generation Strategies



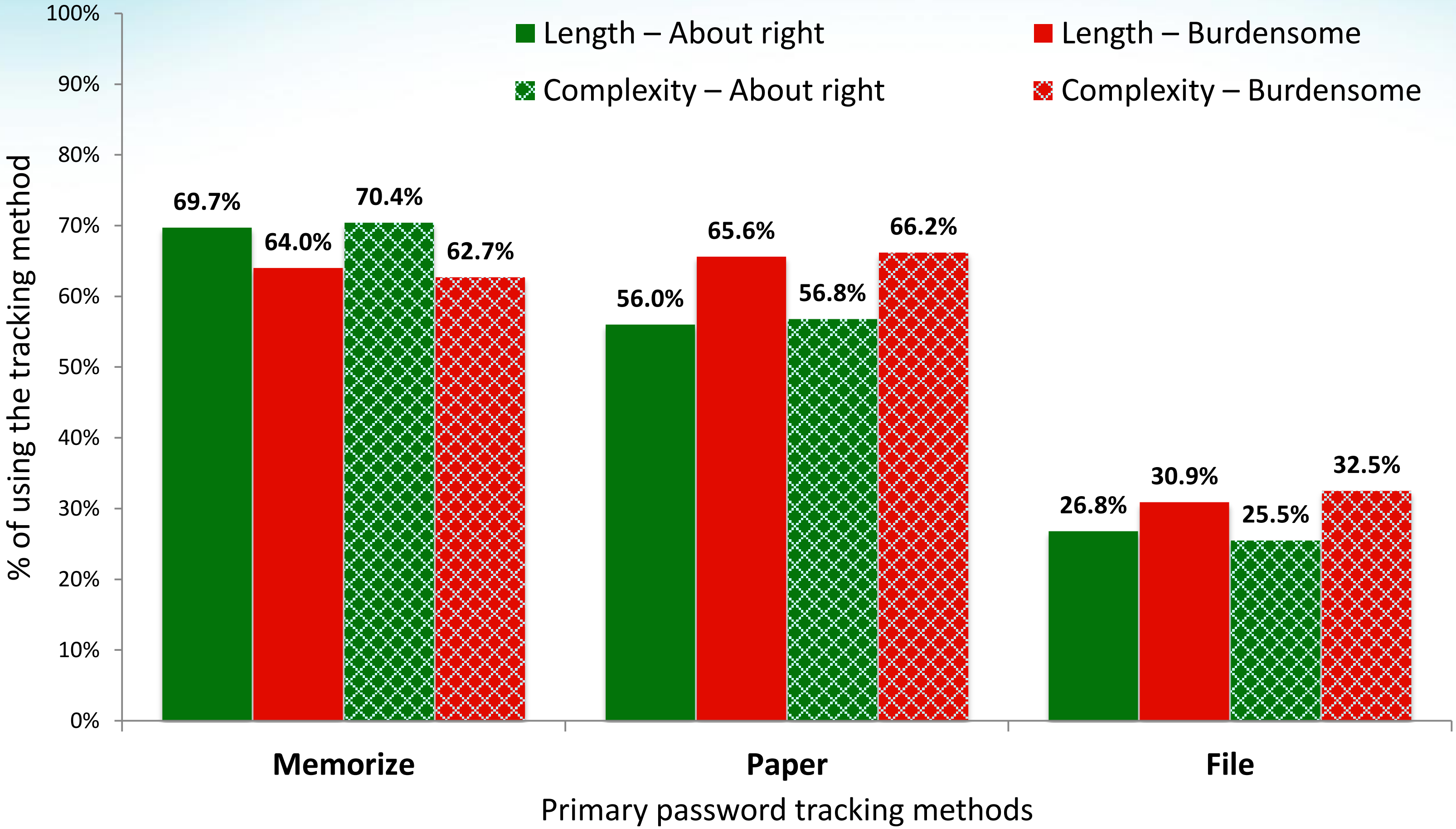
* All comparisons are statistically significant ($p < 0.05$).

Password Generation Considerations



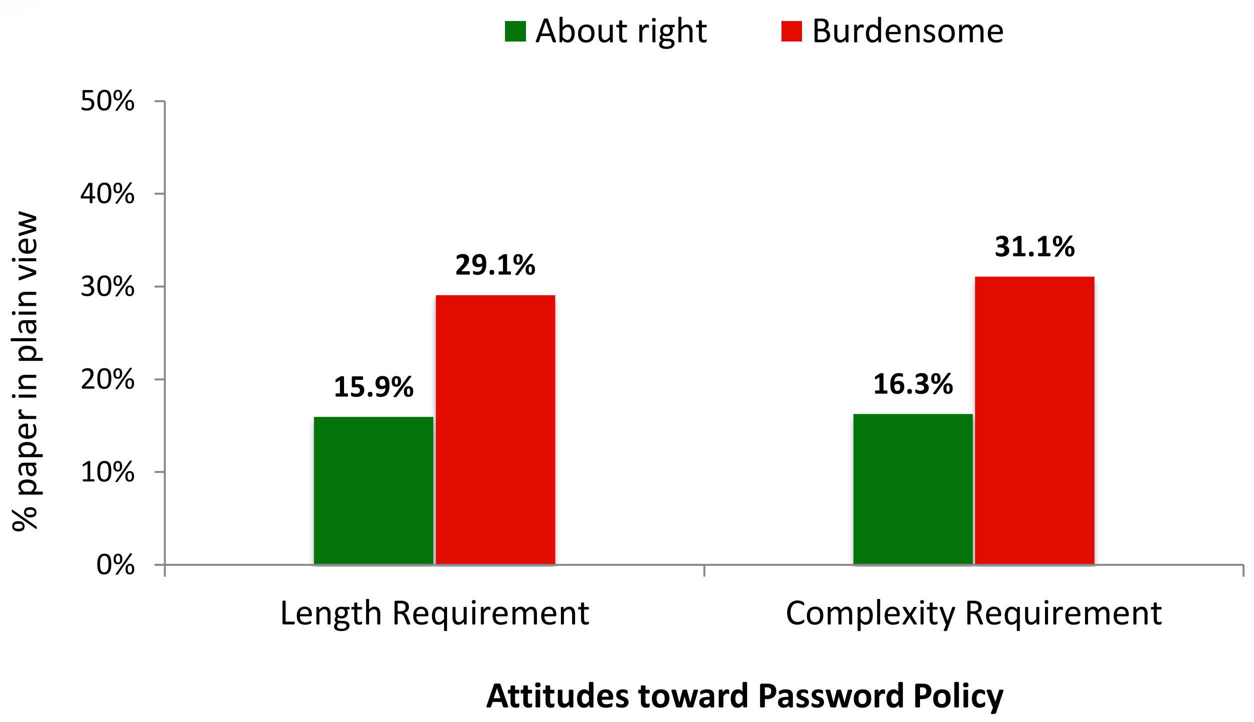
* All comparisons are statistically significant ($p < 0.05$).

Password Maintenance

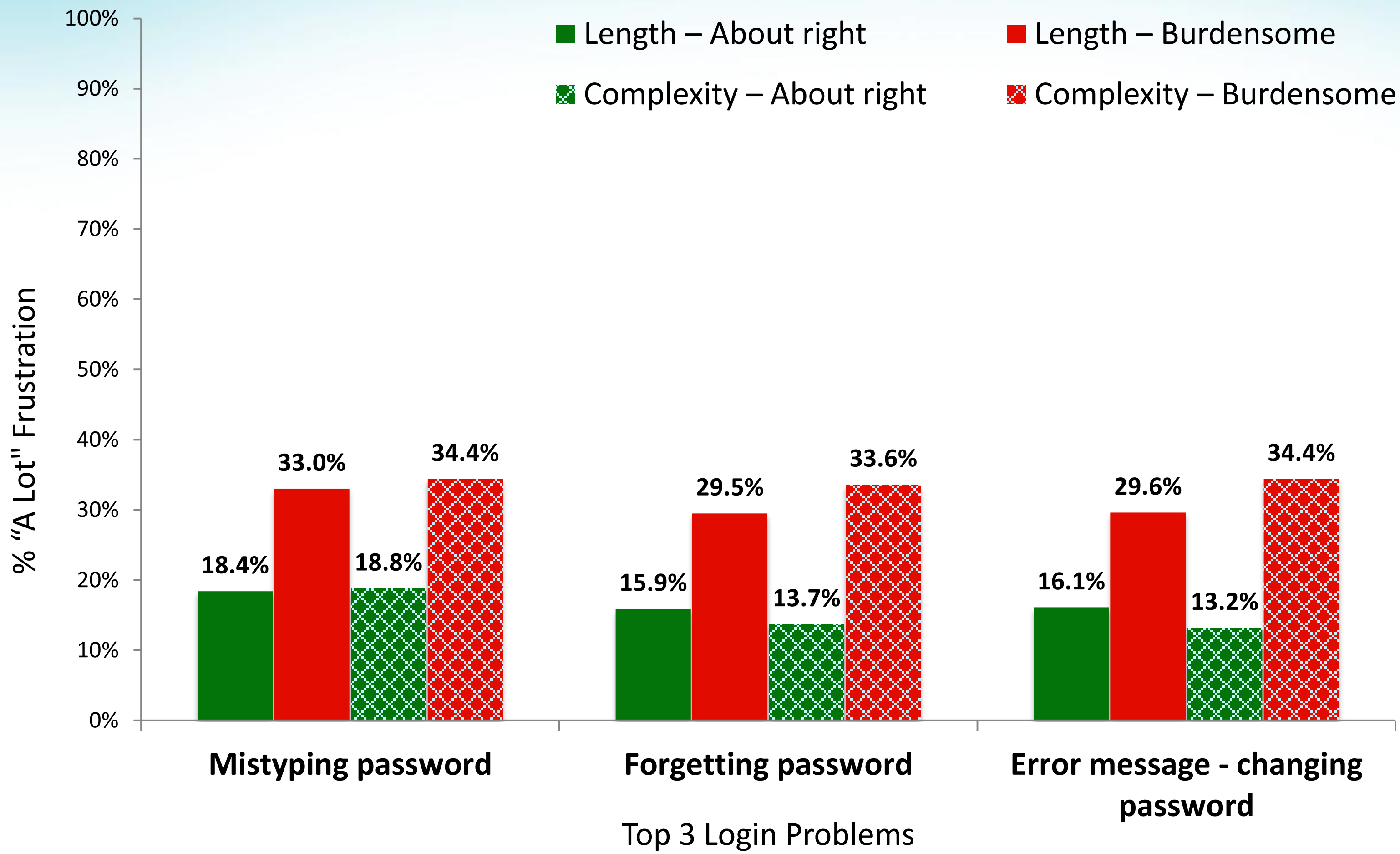


* All comparisons are statistically significant ($p < 0.05$).

Password Tracking – paper in plain view



Authentication Experience



* All comparisons are statistically significant ($p < 0.05$).

What Did 4,500+ People Tell Us?

- *Staff overwhelmed – pushing human cognition limits*
  - different password requirements (length, complexity, expiration)
  - multiple passwords – frustration level significantly related to number of passwords
- *Statistically significant relationships*
  - Attitudes toward organizational security policies
  - Security behaviors and experiences
  - Positive attitudes
    - Compliant and strong passwords more important
    - Write-down passwords less often
    - Less frustration with login problems
    - Better understanding of password security

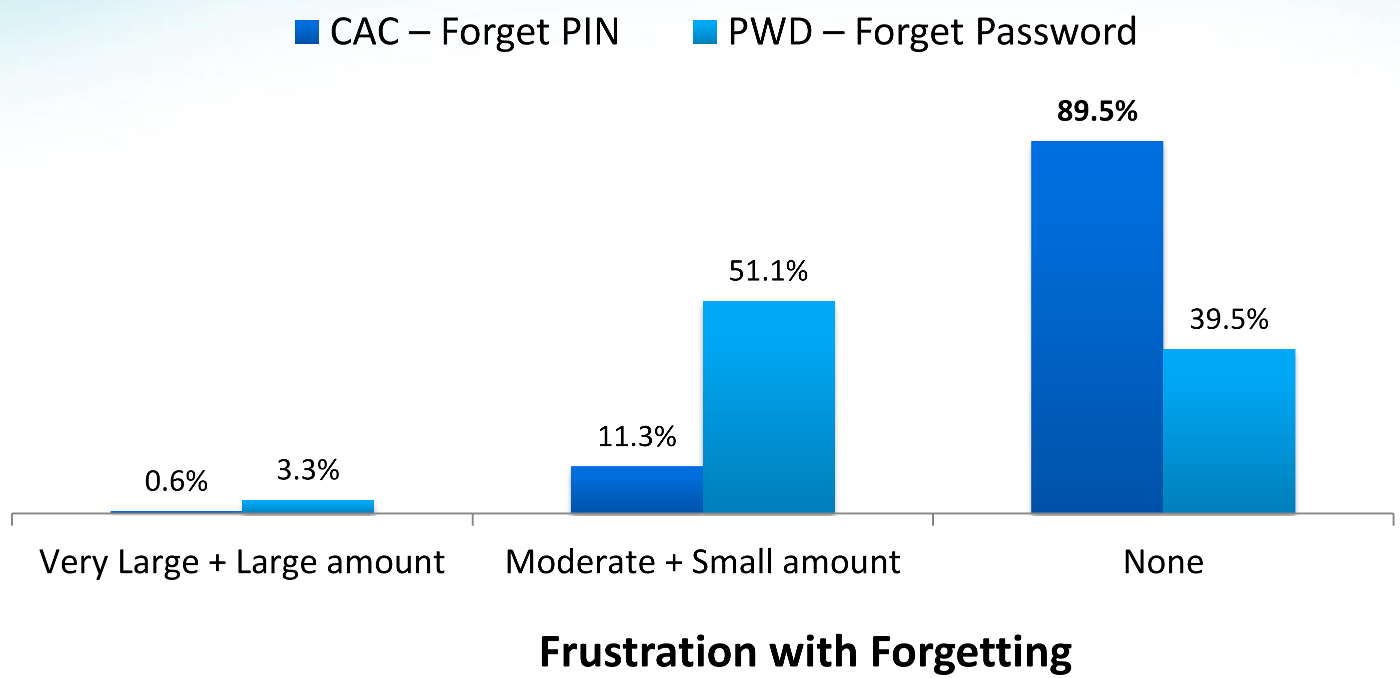
Promising Solution?

- Smart Cards for identification and authentication
- **Security**, multi-factors
  - Something you have – a Smart card
  - Something you know – a PIN
- **Usability**
  - Single sign-on
  - PINs easier to remember and to enter

The case of CAC (Common Access Card)

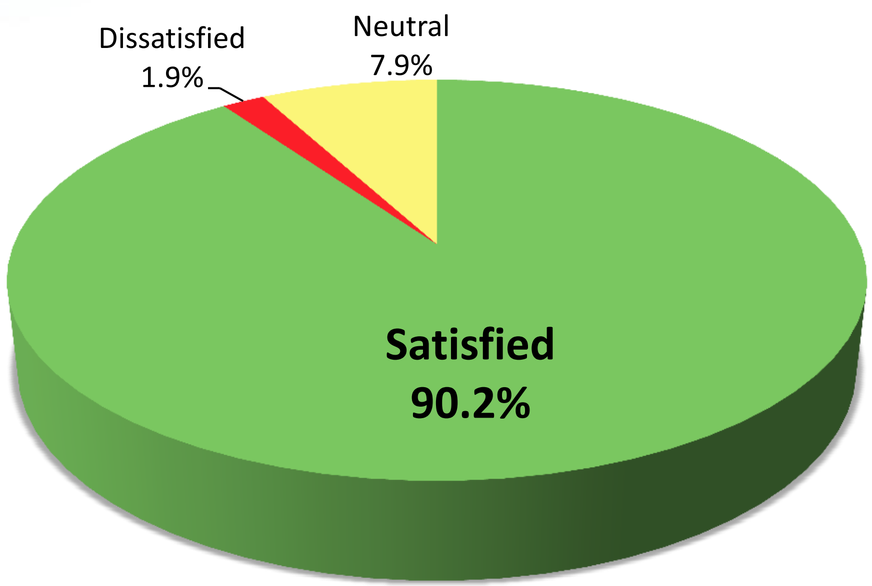
- **CAC**
  - Standard identification for Department of Defense (DoD) personnel
  - Physical access
  - Logical access
- **Online Survey**
  - Anonymous
  - Questions on CAC usage and password management

Authentication Problems – Forgetting



- Statistical significance ($p < 0.05$)
  - More frustration with *Forgetting Password*

User Satisfaction with CAC



Moving Forward

- Better security metrics for user generated passwords
- Usable password requirements
  - Formatting, phrasing, language, feedback
- Potential usability issues with smartcard authentication
- Better organizational security policies
- Direction of causality: *Attitudes* & *Behaviors*
- Promote positive attitudes
- Work and personal password management

References

Choong, Y. Y., Theofanos, M., & Liu, H.-K. (2014). *United States Federal Employees' Password Management Behaviors – A Department of Commerce Case Study,* NISTIR 7991.

Choong, Y. Y. (2014). A cognitive-behavioral framework of user password management lifecycle. In *Human Aspects of Information Security, Privacy, and Trust* (pp. 127-137). Springer International Publishing.

Choong, Y. Y., & Theofanos, M. (2015). What 4,500+ people can tell you–employees' attitudes toward organizational password policy do matter. In *Human Aspects of Information Security, Privacy, and Trust* (pp. 299-310). Springer International Publishing.

Lee, Paul Y., & Choong, Y. Y. (2015). "Human generated passwords–the impacts of password requirements and presentation styles." In *Human Aspects of Information Security, Privacy, and Trust* (pp. 83-94). Springer International Publishing.

Yee-Yin Choong

National Institute of Standards and Technology
Gaithersburg, MD, USA
Yee-yin.choong@nist.gov