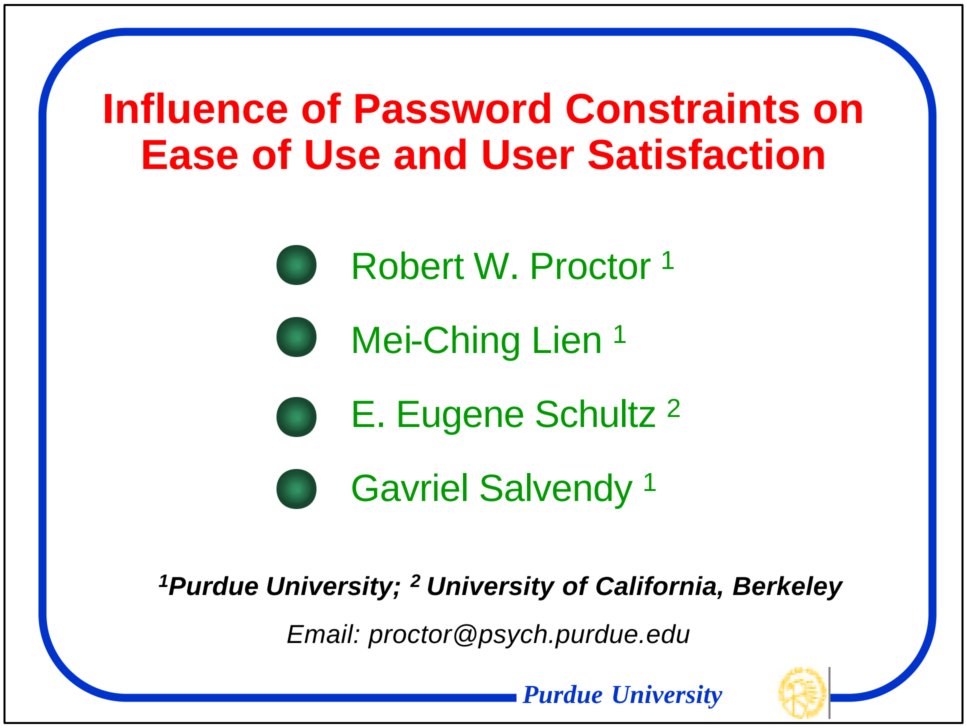
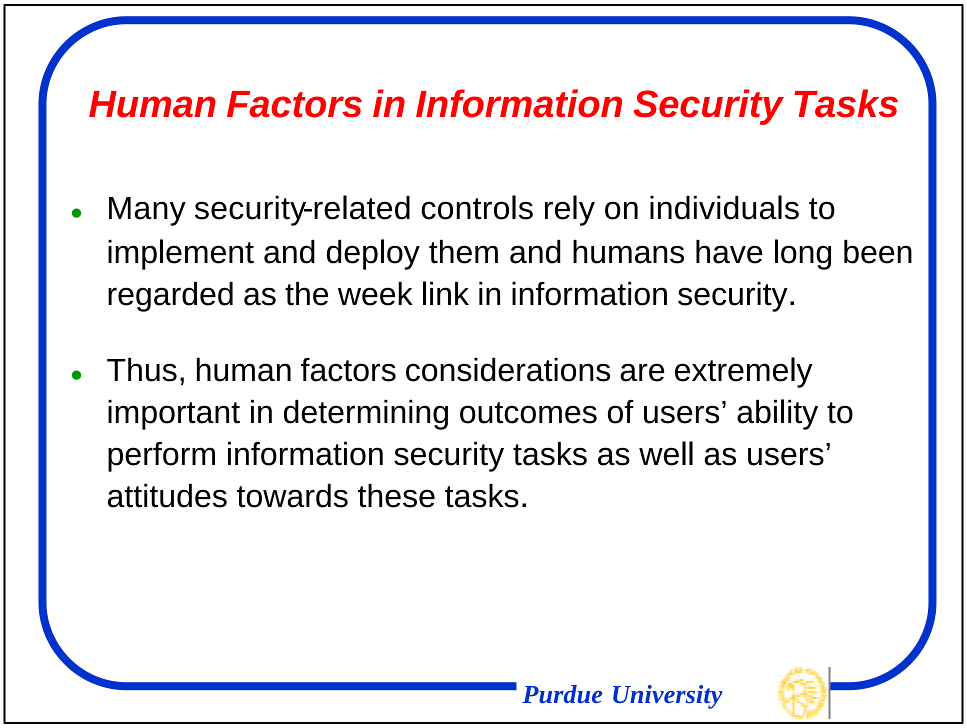


Influence of Password Constraints on Ease of Use and User Satisfaction

- Robert W. Proctor [1]
- Mei-Ching Lien [1]
- E. Eugene Schultz [2]
- Gavriel Salvendy [1]

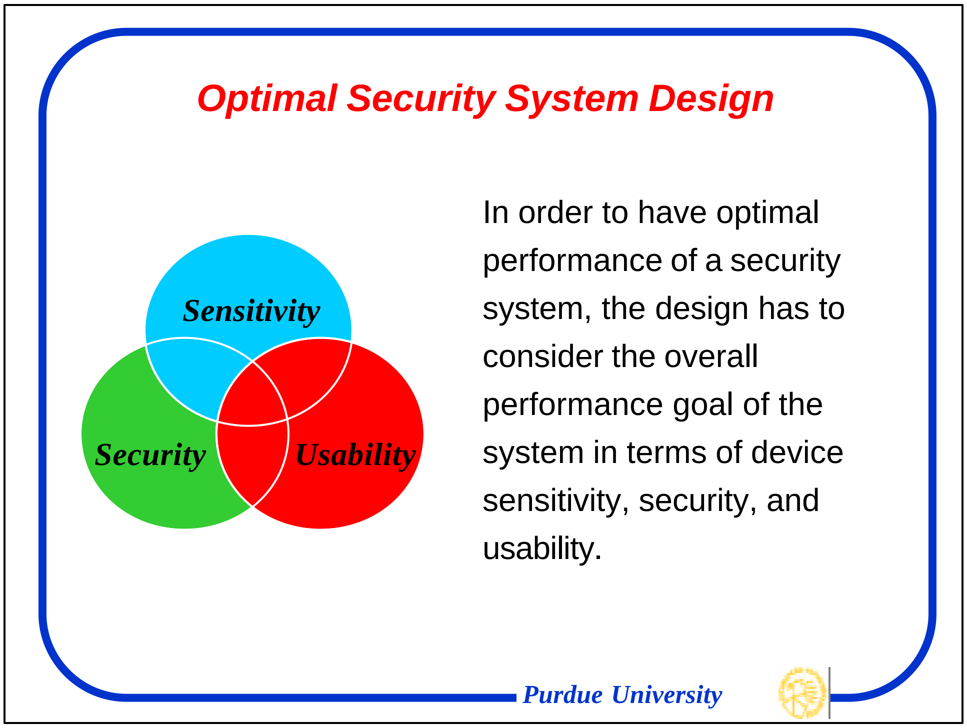
[1]Purdue University; [2] University of California, Berkeley

Email: proctor@psych.purdue.edu



Human Factors in Information Security Tasks

- Many security-related controls rely on individuals to implement and deploy them and humans have long been regarded as the week link in information security.
- Thus, human factors considerations are extremely important in determining outcomes of users’ ability to perform information security tasks as well as users’ attitudes towards these tasks.

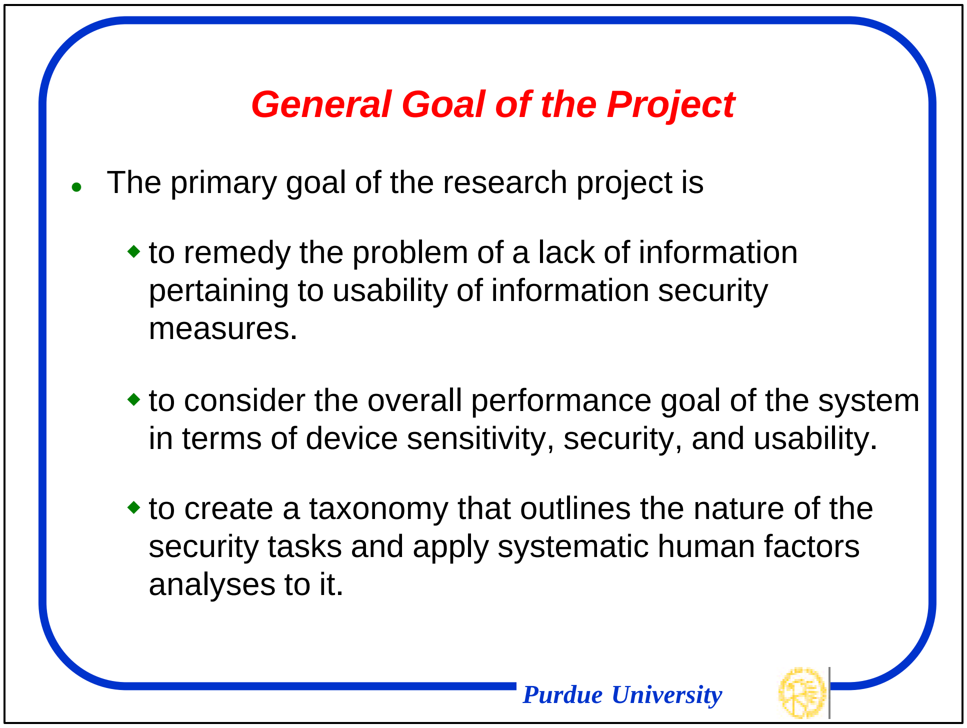


Optimal Security System Design

Sensitivity
Security
Usability

In order to have optimal performance of a security system, the design has to consider the overall performance goal of the system in terms of device sensitivity, security, and usability.

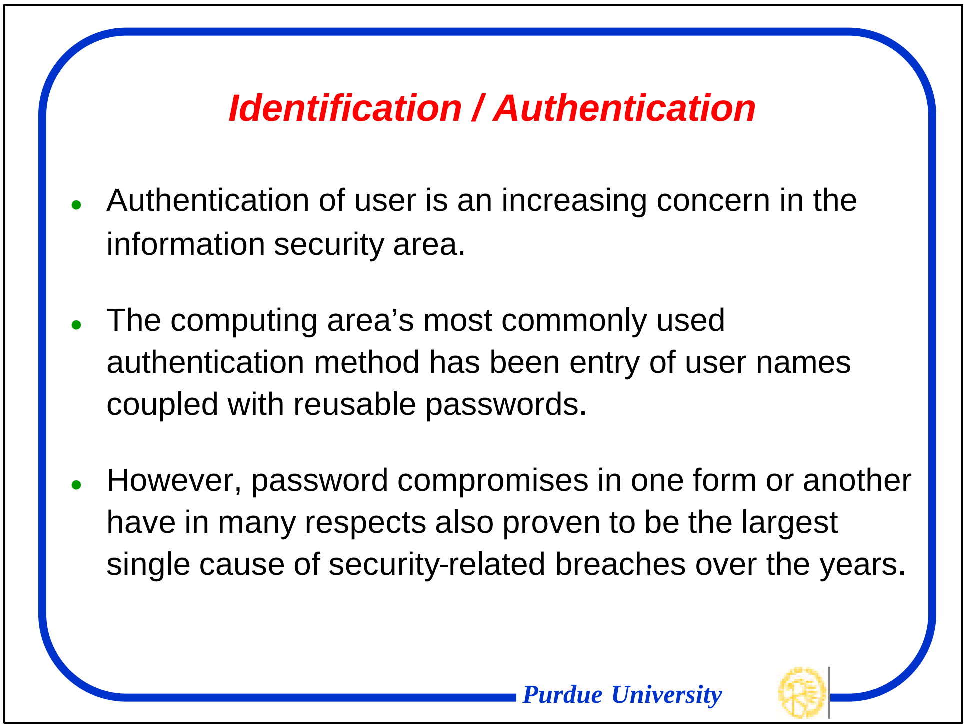
Purdue University



General Goal of the Project

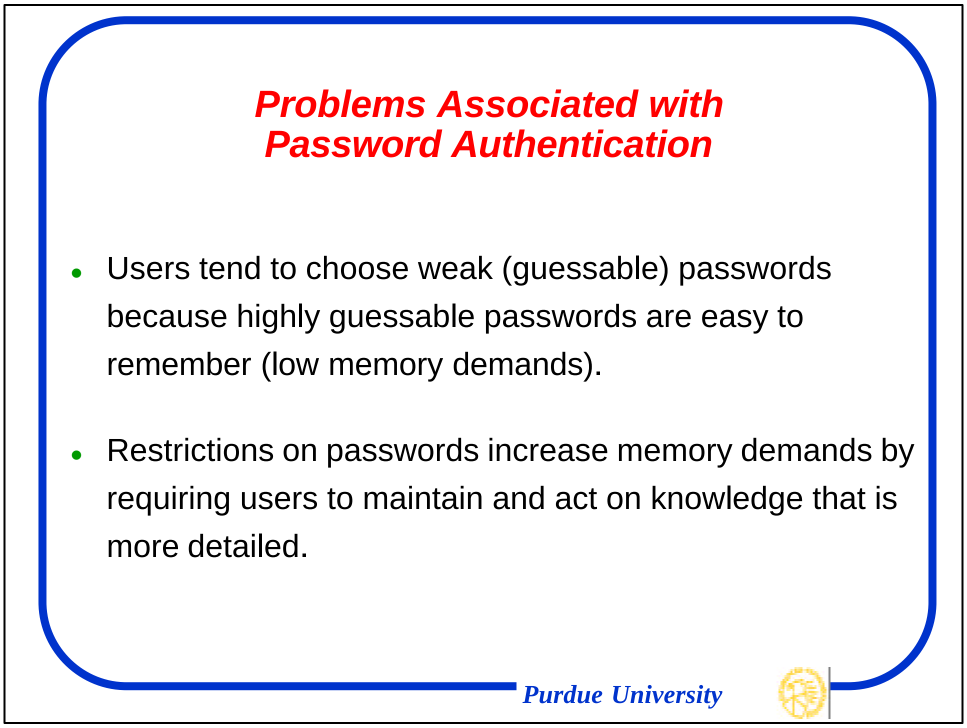
- The primary goal of the research project is
  - to remedy the problem of a lack of information pertaining to usability of information security measures.
  - to consider the overall performance goal of the system in terms of device sensitivity, security, and usability.
  - to create a taxonomy that outlines the nature of the security tasks and apply systematic human factors analyses to it.

Purdue University



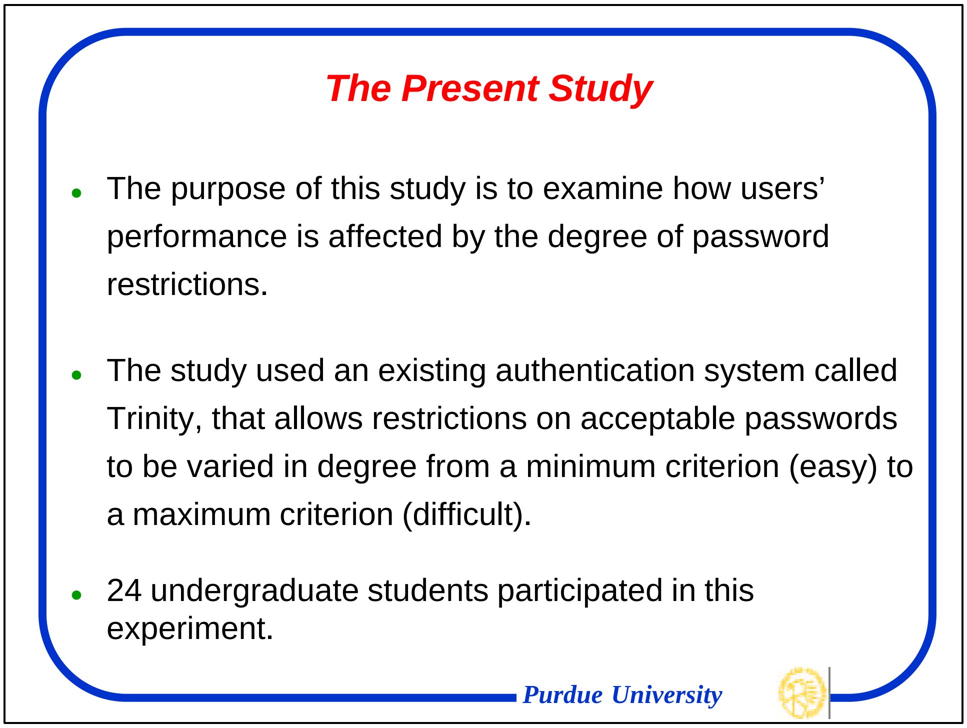
Identification / Authentication

- Authentication of user is an increasing concern in the information security area.
- The computing area's most commonly used authentication method has been entry of user names coupled with reusable passwords.
- However, password compromises in one form or another have in many respects also proven to be the largest single cause of security-related breaches over the years.



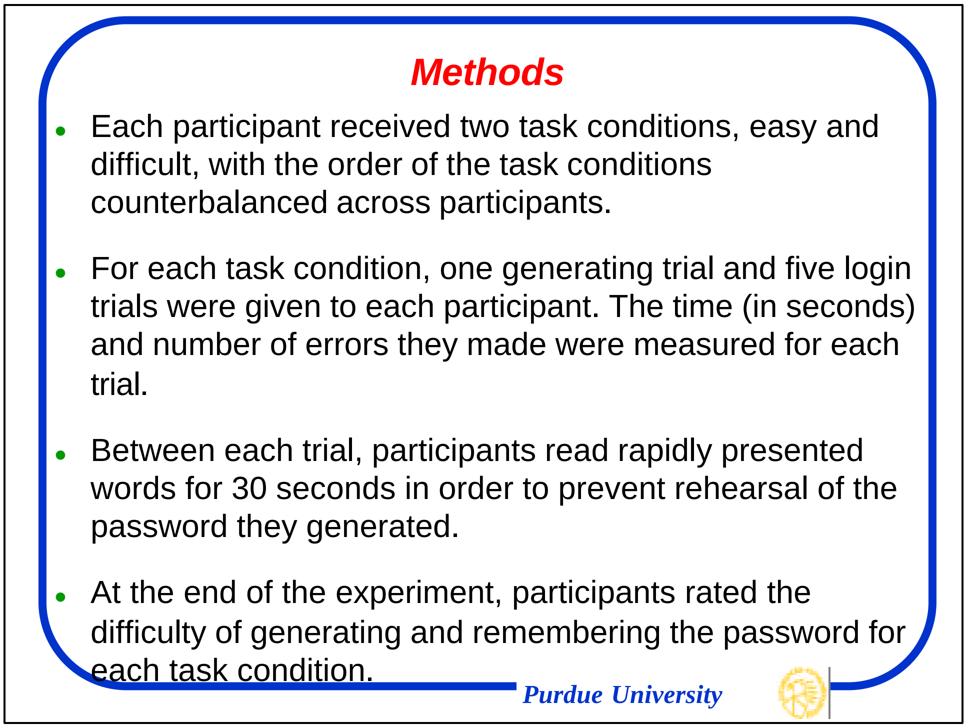
Problems Associated with Password Authentication

- Users tend to choose weak (guessable) passwords because highly guessable passwords are easy to remember (low memory demands).
- Restrictions on passwords increase memory demands by requiring users to maintain and act on knowledge that is more detailed.



The Present Study

- The purpose of this study is to examine how users' performance is affected by the degree of password restrictions.
- The study used an existing authentication system called Trinity, that allows restrictions on acceptable passwords to be varied in degree from a minimum criterion (easy) to a maximum criterion (difficult).
- 24 undergraduate students participated in this experiment.

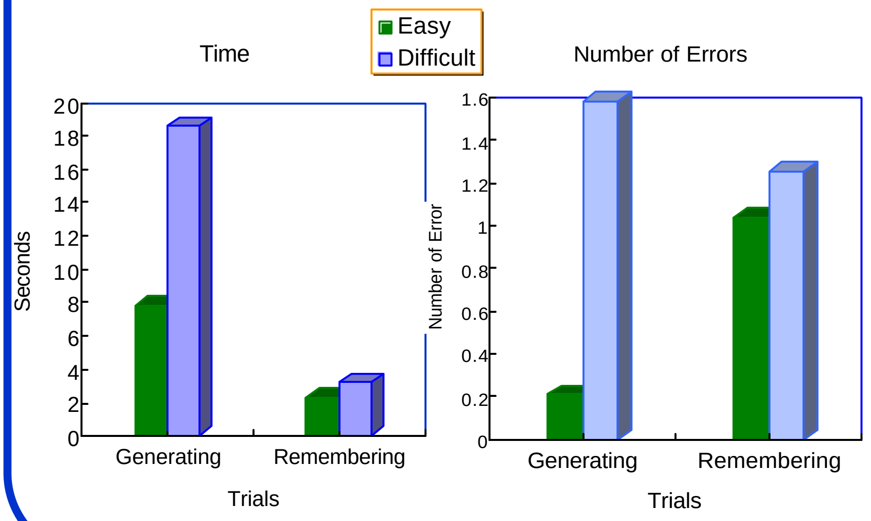


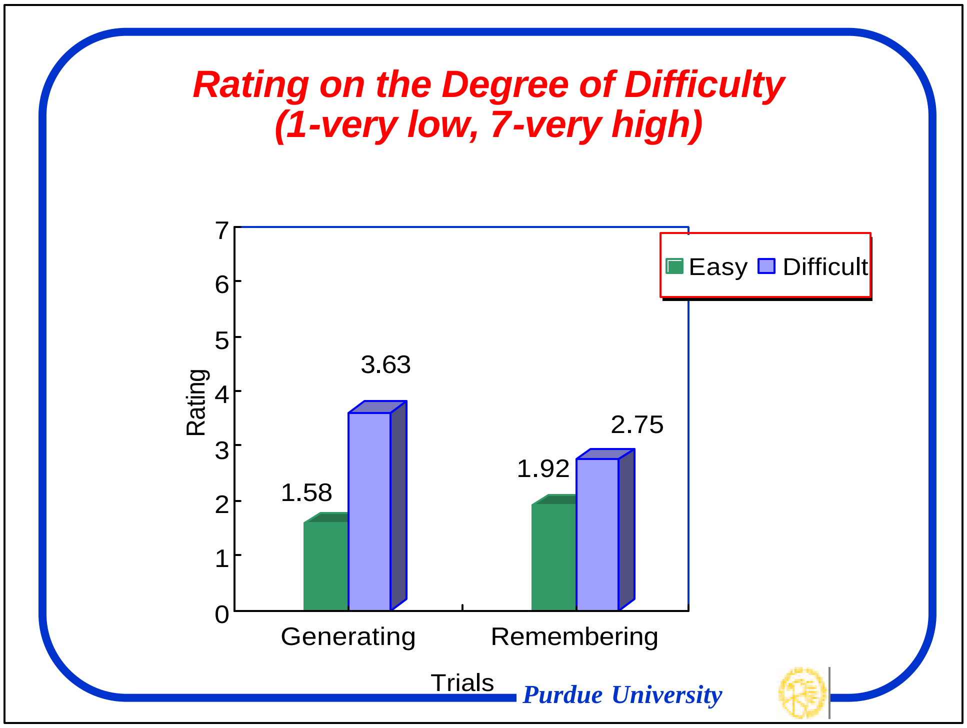
Methods

- Each participant received two task conditions, easy and difficult, with the order of the task conditions counterbalanced across participants.
- For each task condition, one generating trial and five login trials were given to each participant. The time (in seconds) and number of errors they made were measured for each trial.
- Between each trial, participants read rapidly presented words for 30 seconds in order to prevent rehearsal of the password they generated.
- At the end of the experiment, participants rated the difficulty of generating and remembering the password for each task condition.

- The restrictions for each condition:
  - Easy task condition
    - Minimum length at least 5 characters
  - Difficult task condition
    - Minimum length at least 5 characters
    - Must contain uppercase
    - Must contain lowercase
    - Must contain a number
    - Must not repeat a character 2 times in a row
    - Must not contain 2 characters from the login name (which was the last name for all participants)

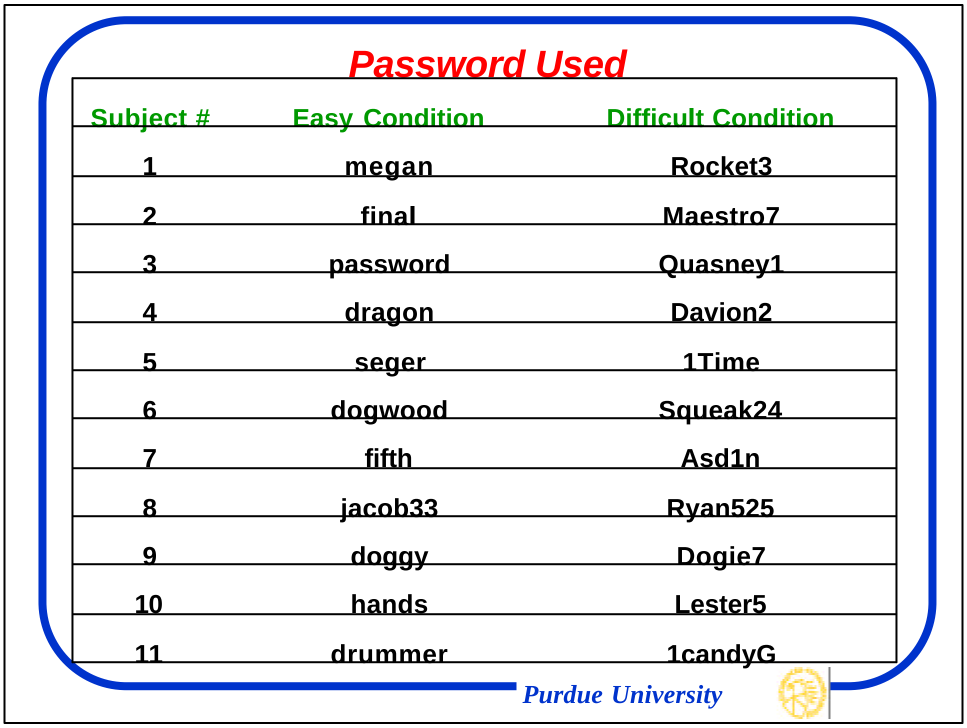
Results





Rating on the Degree of Difficulty (1-very low, 7-very high)

Purdue University



Password Used

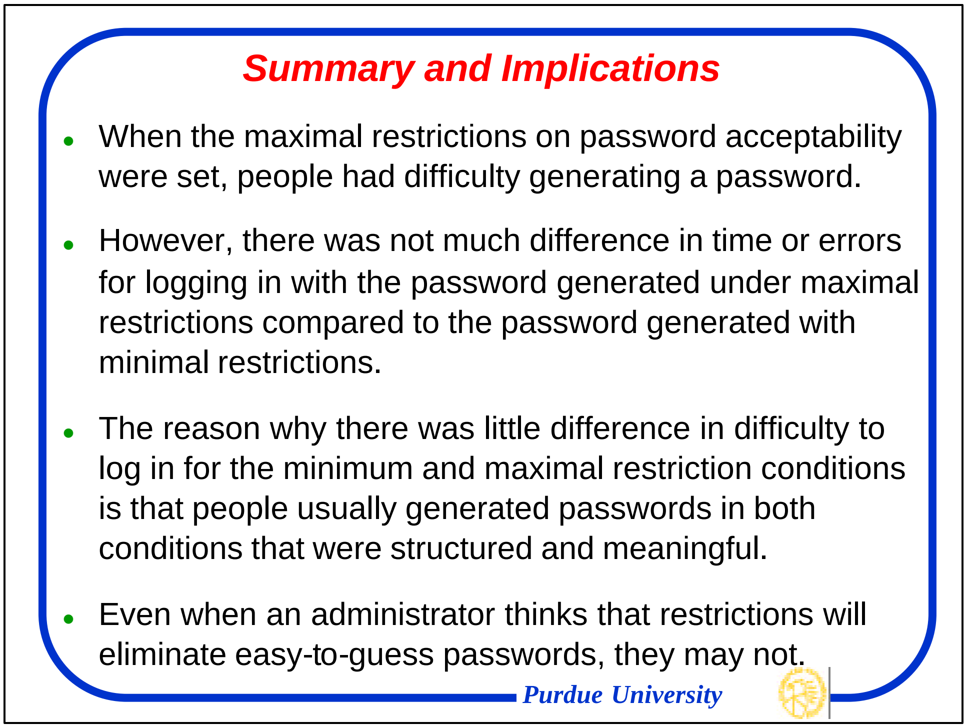
Subject #	Easy Condition	Difficult Condition
1	megan	Rocket3
2	final	Maestro7
3	password	Quasney1
4	dragon	Davion2
5	seger	1Time
6	dogwood	Squeak24
7	fifth	Asd1n
8	jacob33	Ryan525
9	doggy	Dogie7
10	hands	Lester5
11	drummer	1candyG

Purdue University

12	666girly	6aGirl
13	271toaster	271Toast
14	meijer	Fender8
15	pusher9	Noland8
16	miles	Mito1
17	anarchy	Total1
18	goette	abcd4E
19	corona	April1
20	mikey	Dra4230
21	kishm	Love5
22	mike2	recoN23
23	chewy	Chewy3
24	jjjjj	boscO9

Password Characteristics

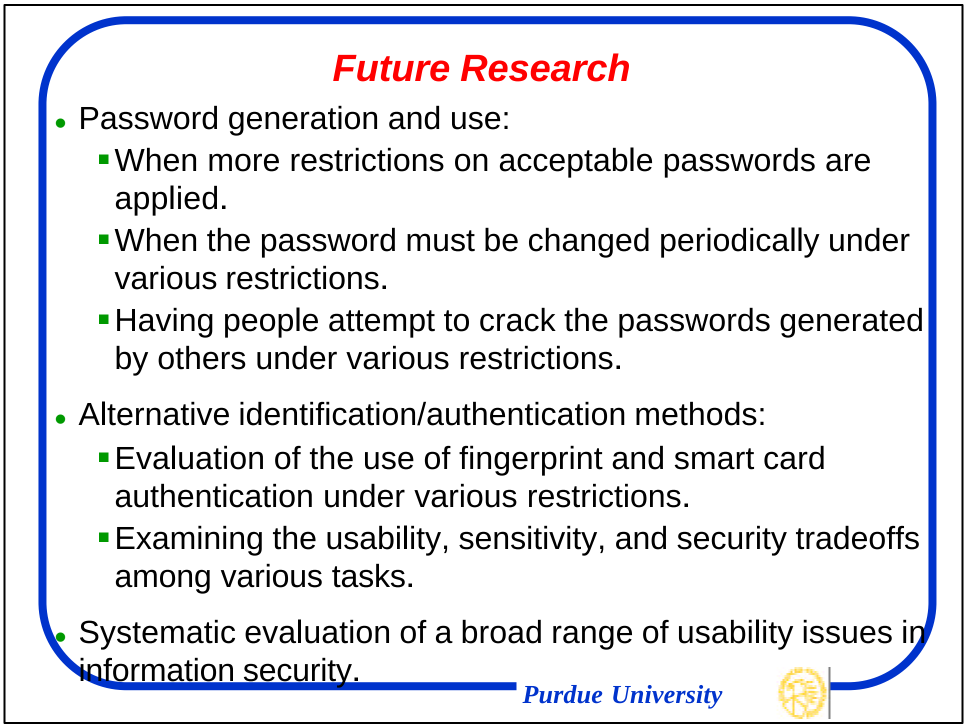
- The passwords people used followed simple rules, even when the maximal restrictions on password acceptability allowed by Trinity were implemented.
- Personal information was used in many cases, regardless of whether the task condition was easy or difficult.
- Although there were a lot of restrictions on the password generation for the difficult condition, people usually devised a simple password that likely would be easy to crack.



Summary and Implications

- When the maximal restrictions on password acceptability were set, people had difficulty generating a password.
- However, there was not much difference in time or errors for logging in with the password generated under maximal restrictions compared to the password generated with minimal restrictions.
- The reason why there was little difference in difficulty to log in for the minimum and maximal restriction conditions is that people usually generated passwords in both conditions that were structured and meaningful.
- Even when an administrator thinks that restrictions will eliminate easy-to-guess passwords, they may not.

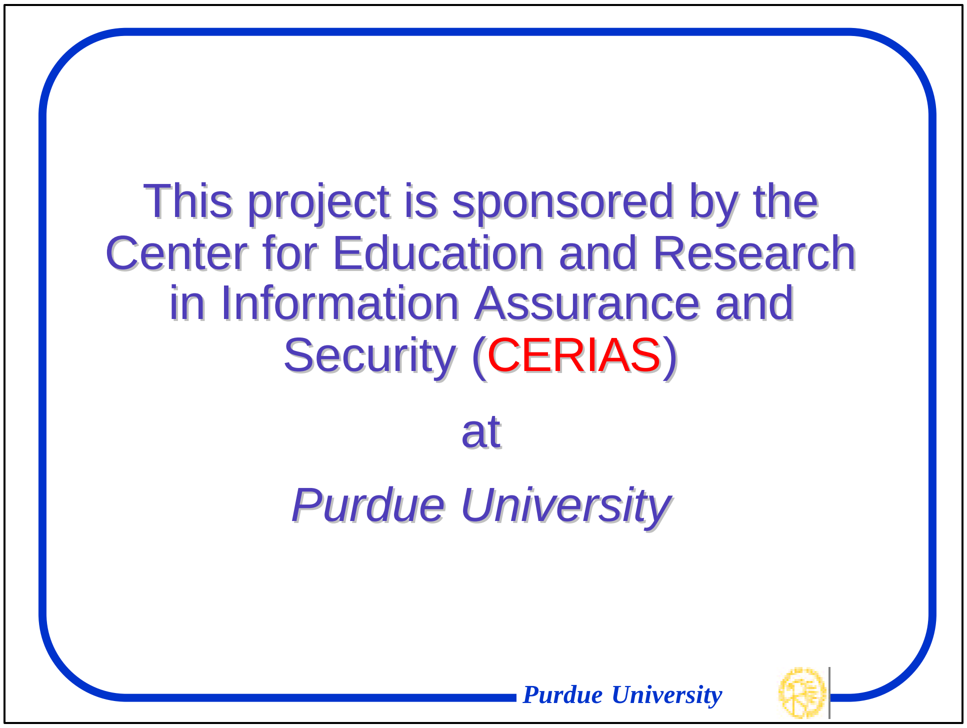
Purdue University



Future Research

- Password generation and use:
  - When more restrictions on acceptable passwords are applied.
  - When the password must be changed periodically under various restrictions.
  - Having people attempt to crack the passwords generated by others under various restrictions.
- Alternative identification/authentication methods:
  - Evaluation of the use of fingerprint and smart card authentication under various restrictions.
  - Examining the usability, sensitivity, and security tradeoffs among various tasks.
- Systematic evaluation of a broad range of usability issues in information security.

Purdue University



This project is sponsored by the Center for Education and Research in Information Assurance and Security (CERIAS)

at

Purdue University