THE UNIVERSITY OF IDAHO

1889

University of Idaho

A LEGACY OF LEADING

The Human Element in Computer Security - Graphical Passcodes as a Means to Create Secure Authentication systems

Steffen Werner
University of Idaho

University of Idaho
A LEGACY OF LEADING

Why Research on User Authentication?

- The applied appeal
  - Growing importance of stored assets
    - Shift to web-based services, cybersecurity
  - Increased need for computer security
    - Increase in attacks
  - Increasing rigor of authentication protocols

Why Research on Passwords?

- The theoretical appeal
  - Ideal scenario for human-technology optimization
  - Quantitative definition of engineering goals
  - Problem open to multiple solutions
  - Large body of relevant psychological literature
    - Different types of memory systems
    - Free recall vs. cued recall vs. recognition tests
    - Visual perception, visual attention, visual memory

Overview of the Talk

- Approaches to authentication
- What makes a good password system?
  - Maximization of actual password entropy
  - Elimination of predictable user choices
  - Elimination of other unsafe user behavior
- Overview of graphical approaches to password systems
- 4 studies evaluating aspects of our new CSA graphical password system against alternative approaches

Current Approaches to Authentication

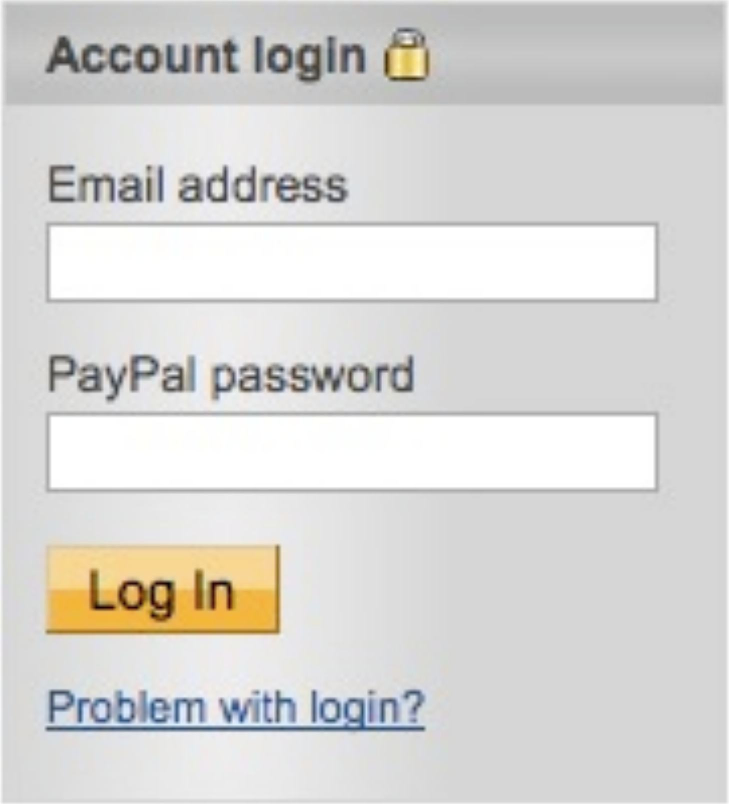
- Passwords
- Token-based authentication
- Biometric authentication
- Behavioral analysis

and combinations through …

- Two-factor (multi-factor) authentication

Password Authentication is Cognitive Authentication

- The user possesses unique knowledge
- Relies on memory storage of information*
- Problems: forgetting, phishing, guessing, theft (shoulder surfing)



Account login

Email address

PayPal password

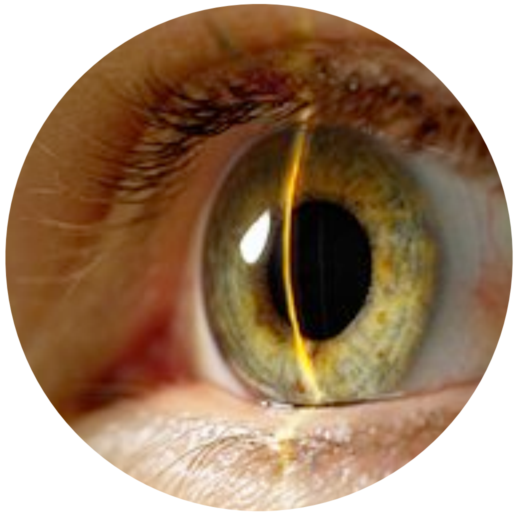
**unless written down*

Hardware Token-based Authentication

- Token identifies user (passport)
- One-time passwords (OTP)
- Usually used in combination with pin or other password
- Problems: theft, loss, failure, difficult to replace (time, cost)

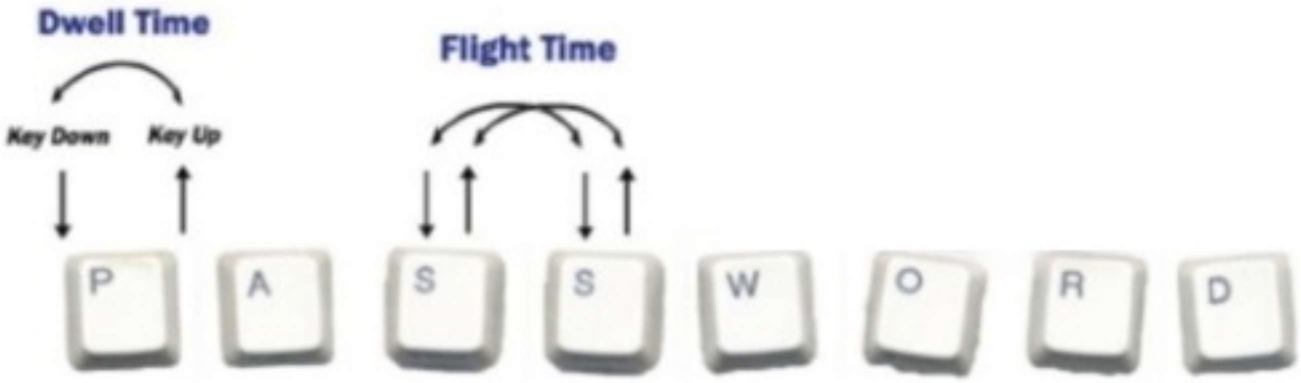
Biometric Authentication

- Authentication through a physical characteristic of the user
- Examples: fingerprint, retinal scan, iris scan, vascular patterns, voice recognition, DNA
- Problems: cost, limited replaceability, user acceptance, stability of biometric parameters



Authentication through Behavioral Analysis

- Authentication through a unique behavioral patter of the user
- Keystroke, mouse, or signature dynamics, voice recognition, gate, posture, etc.
- Problems: Changes (fatigue, illness), injury, aging



What Makes a Good Password?

- Increase effective password entropy
- Decrease forgetting of passwords
- Enable safe and fast entry of password
- The current **password problem:** Inverse relation between safety of password and memorability

Theoretical vs. Effective Entropy in Alphanumeric Passwords

$$H(X) = -\sum_{i=1}^{n} p(X_i) log_2 p(X_i)$$

- Theoretical password space = #chars $^{\text{password length}}$
- Human users restrict their password choices to a small subset of possible passwords, reducing effective entropy
  - preference for short passwords (6-7 characters)
  - use of lower-case letters or digits only
  - use of dictionary words and personally relevant dates

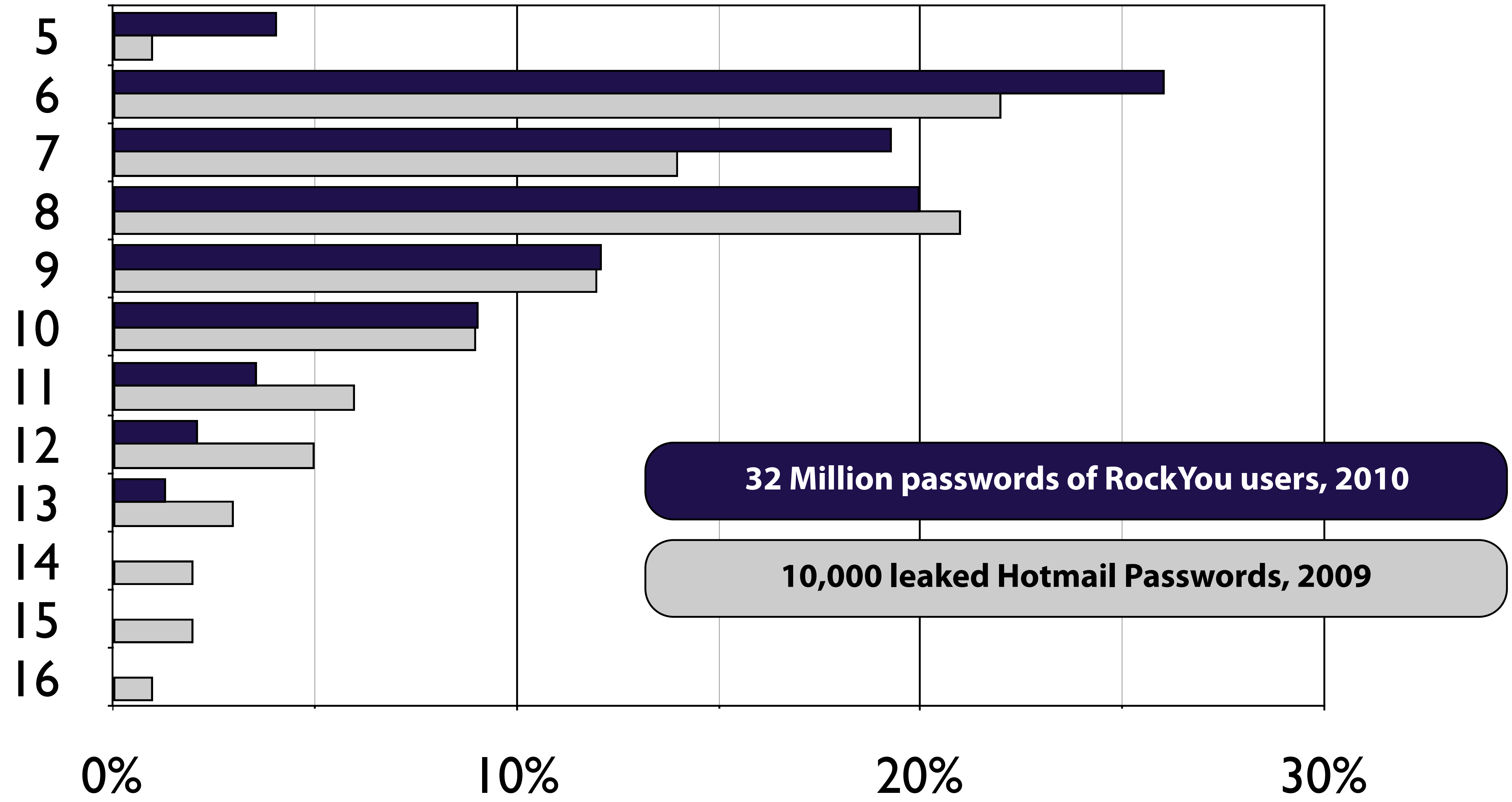
RockYou Password Leak

The top 20 passwords of 32 million

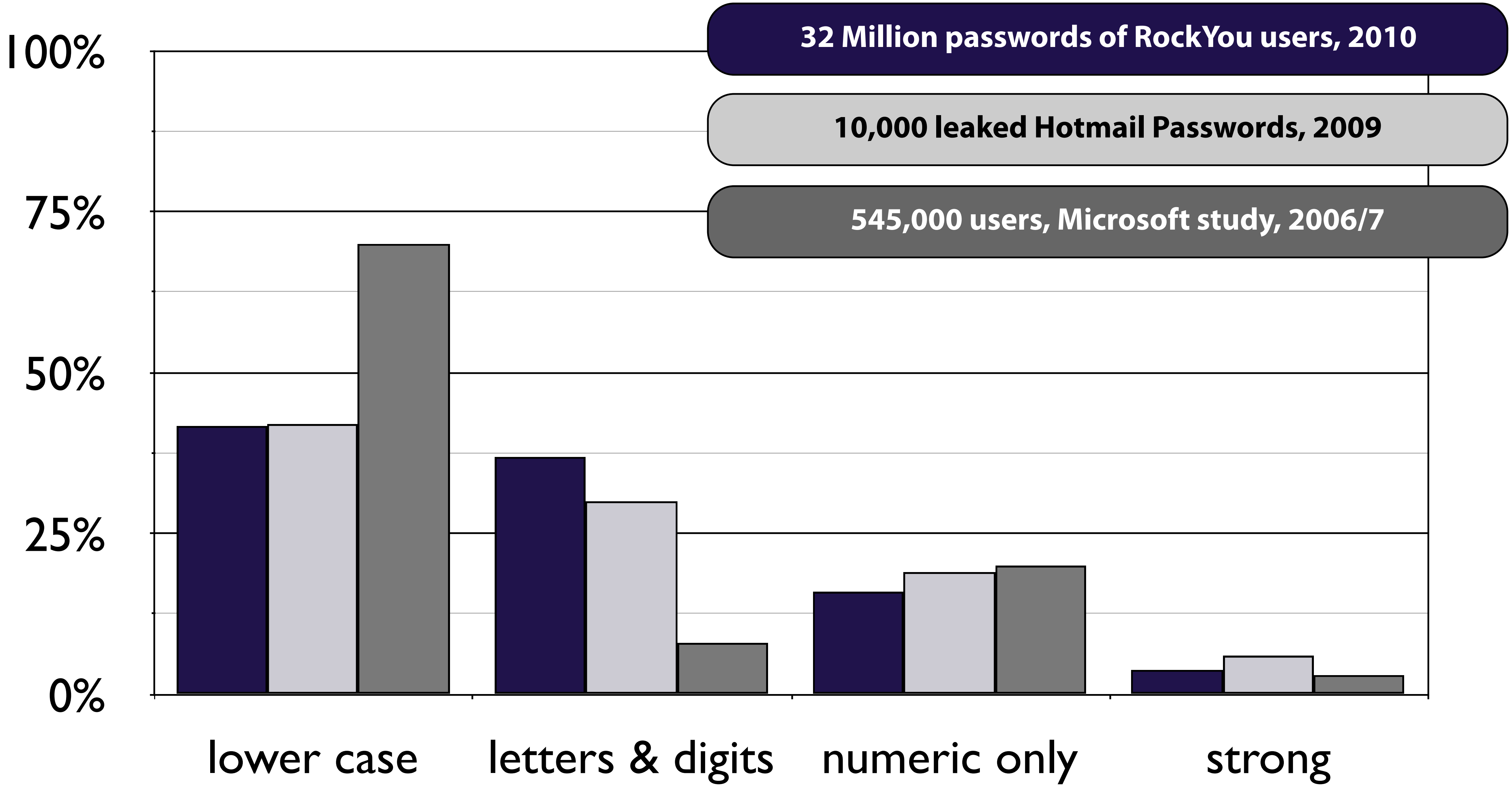
Rank	password	total
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

Imperva (2010). Consumer Password Worst Practices

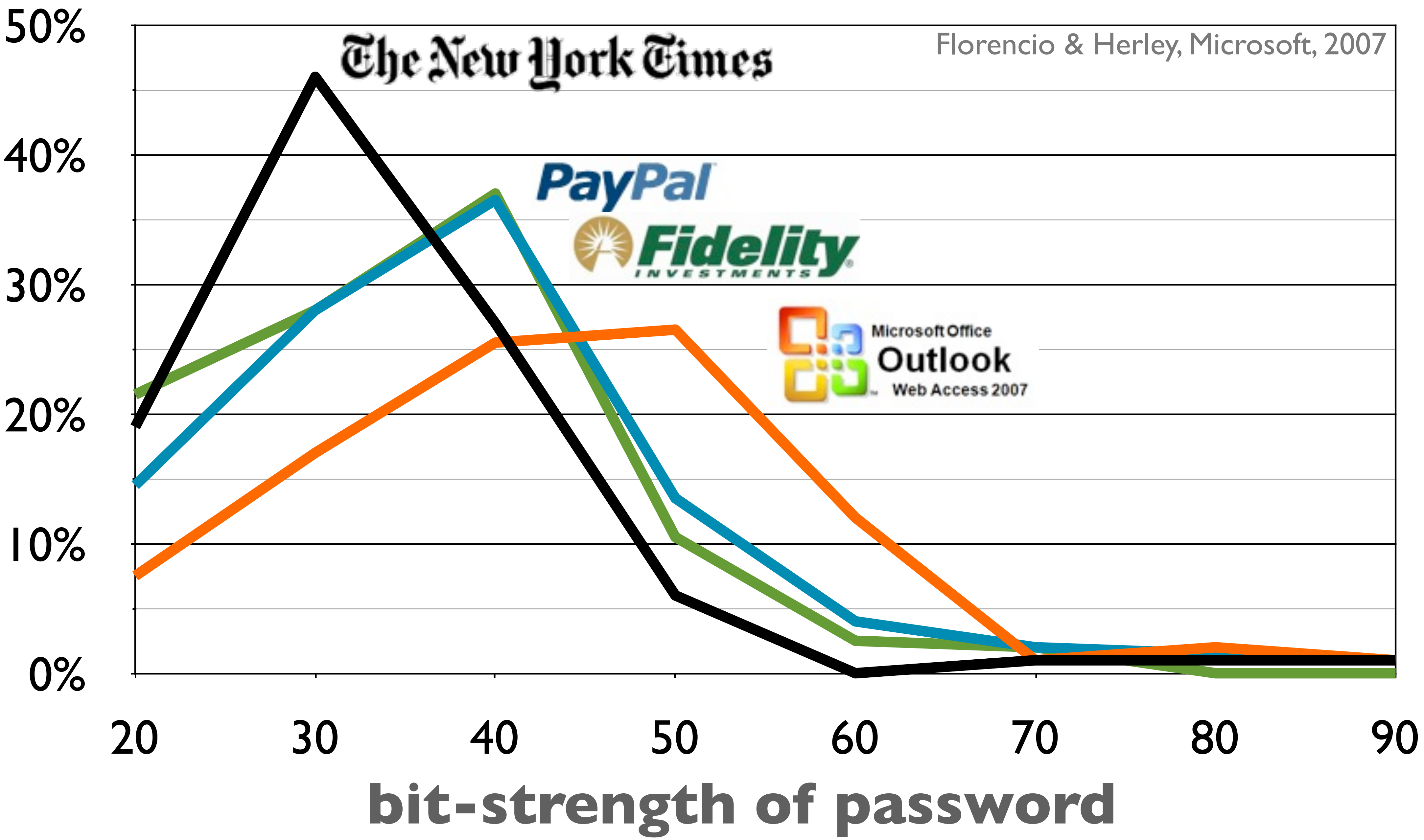
Distribution of Password Lengths



Distribution of Password Types



Theoretical bit-strength for different logins



Florencio & Herley, Microsoft, 2007

Where do Security Policies come from? Analysis of 75 different (large) websites

Dinei Florencio and Cormac Herley, Microsoft, 2010

- greater security demands not a factor
- size of site, num of users, value of assets protected and attack frequency show no correl with strength
- sites with most restrictive password policies don’t have greater security concerns, they are simply better insulated from the consequences of poor usability
- median password policy strengths:
  .com sites = 19.9 bits
  banks = 31.0 bits
  .edu = 43.7 bits and .gov = 47.6 bits

What about Password Forgetting?

- Estimate of 4.3% of active Yahoo users forget their password within a three month period
- Company statistics are not publicly available
- User strategies to fight forgetting
  - Choice of meaningful passwords
  - Password reuse between multiple sites
  - Password reset as a common procedure
  - External storage of password

Summary of Current Status

- **Inverse relation between security and memorability for alphanumeric passwords**
  - Users choose easily predictable passwords
  - Users can't remember secure (complex and random) passwords
  - Attempts to enforce secure password practice are often circumvented
    - Content requirements ➠ Passwords are written down
    - Change regimes ➠ Highly similar passwords

- **Allowing user selection decreases security**

The Promise of Graphical Passcodes

- Visual material is easy to remember - **Picture Superiority Effect**
  - Shepard (1967). Recognition memory for words, sentences, and pictures showed superiority of pictures
- Visual long-term memory has a vast capacity
  - Standing et al (1970): 2,560 pictures tested
  - Standing (1973): up to 10,000 pictures tested
- Visual long-term memory shows little decay
  - Nickerson (1968): Retention tested up to 1 year

Graphical Passcodes: The Pesky Details 1

Picture superiority requires **heterogeneous set of stimuli**

Goldstein & Chance (1970) testing memory for faces, snowflakes and crystals with poor memory performance

http://www.its.caltech.edu/~atomic/snowcrystals

Graphical Passcodes: The Pesky Details II

Visual information is often **not encoded at all**

Change blindness (Rensink et al., 1997; Simons and Levin, 1997)

Graphical Passcodes: The Pesky Details II

Visual information is often **not encoded at all**

Change blindness (Rensink et al., 1997; Simons and Levin, 1997)

Graphical Passcodes: The Pesky Details III

Human observers extract **gist of pictures rapidly** and **remember gist well**

Meaning of a scene can be identified within 0.1s (Potter, 1975)

Graphical Passcodes: The Pesky Details IV

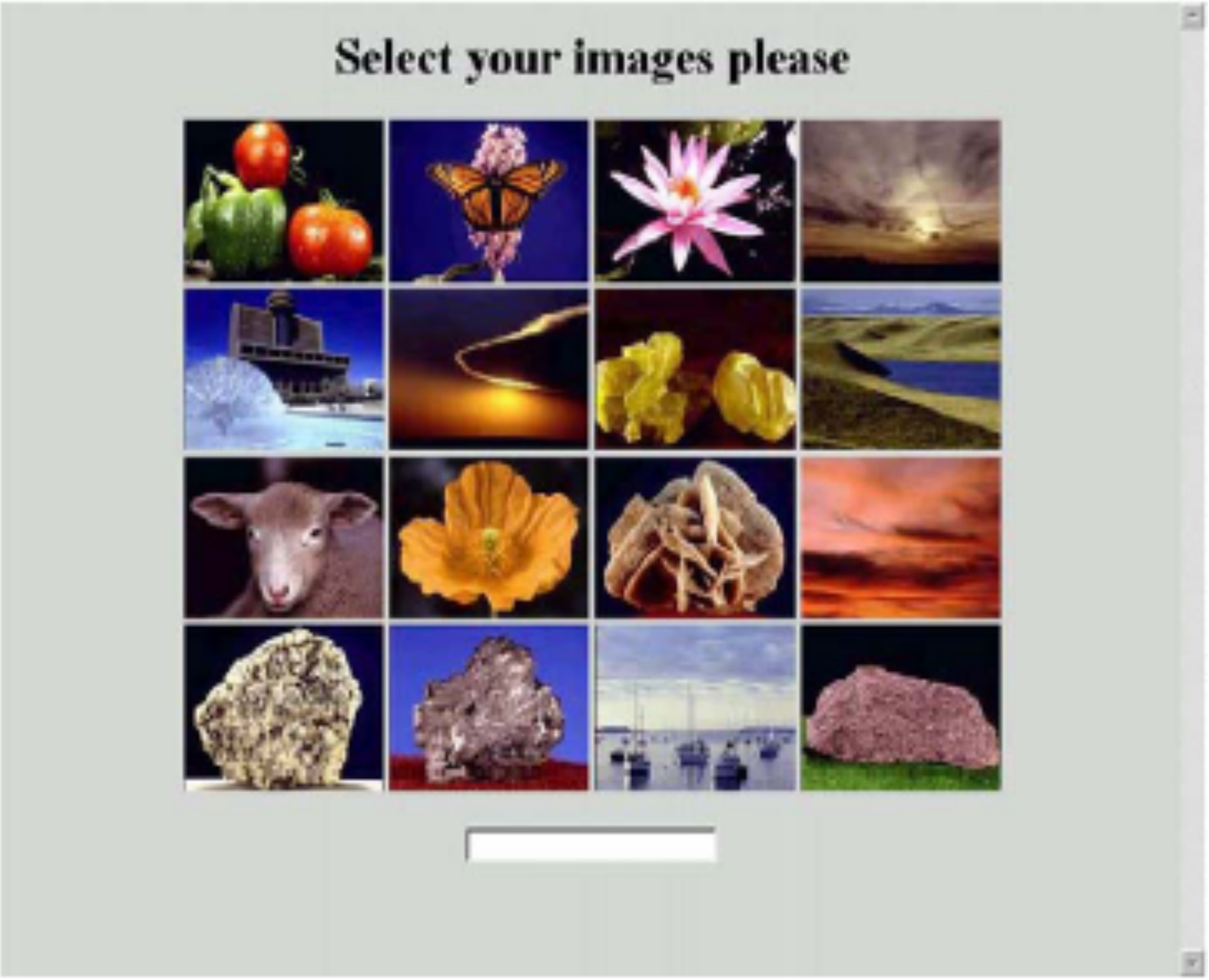
Object interactions and consistency within a scene guide scene interpretation

Coherent scenes are easier to interpret (Biederman et al.,1974)

Main Types of Graphical Authentication

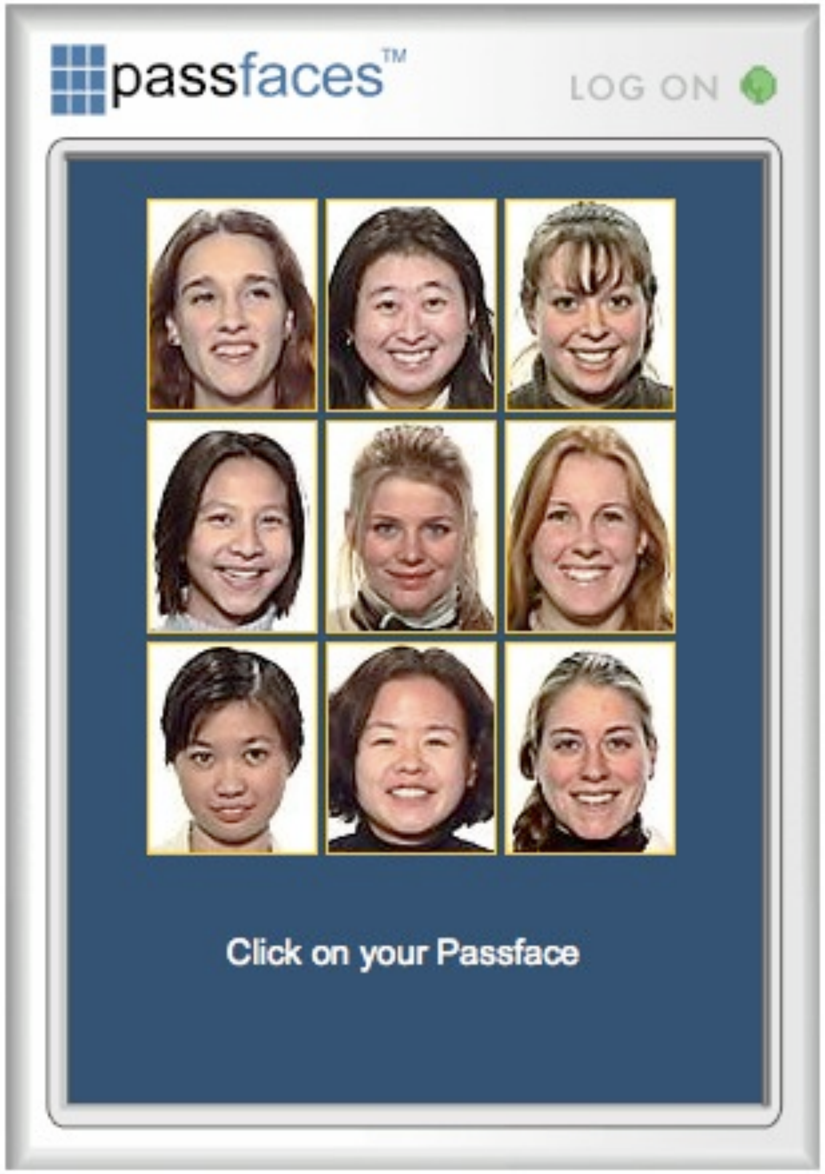
- **Visual recognition paradigm**
  - Enrollment: User learns password image set
  - Authentication: User has to select the presented images
- **Spatial passcodes - cued recall**
  - Enrollment: User learns sequence of locations within a visual scene / a set of images
  - Authentication: User has to replay the sequence
- **Gestural passcodes - cued or free recall**
  - User has to reproduce a specific set of doodles/signature
  - **Might use more procedural memory**

VIP (De Angeli et al., 2005)
“select the images from your password set”



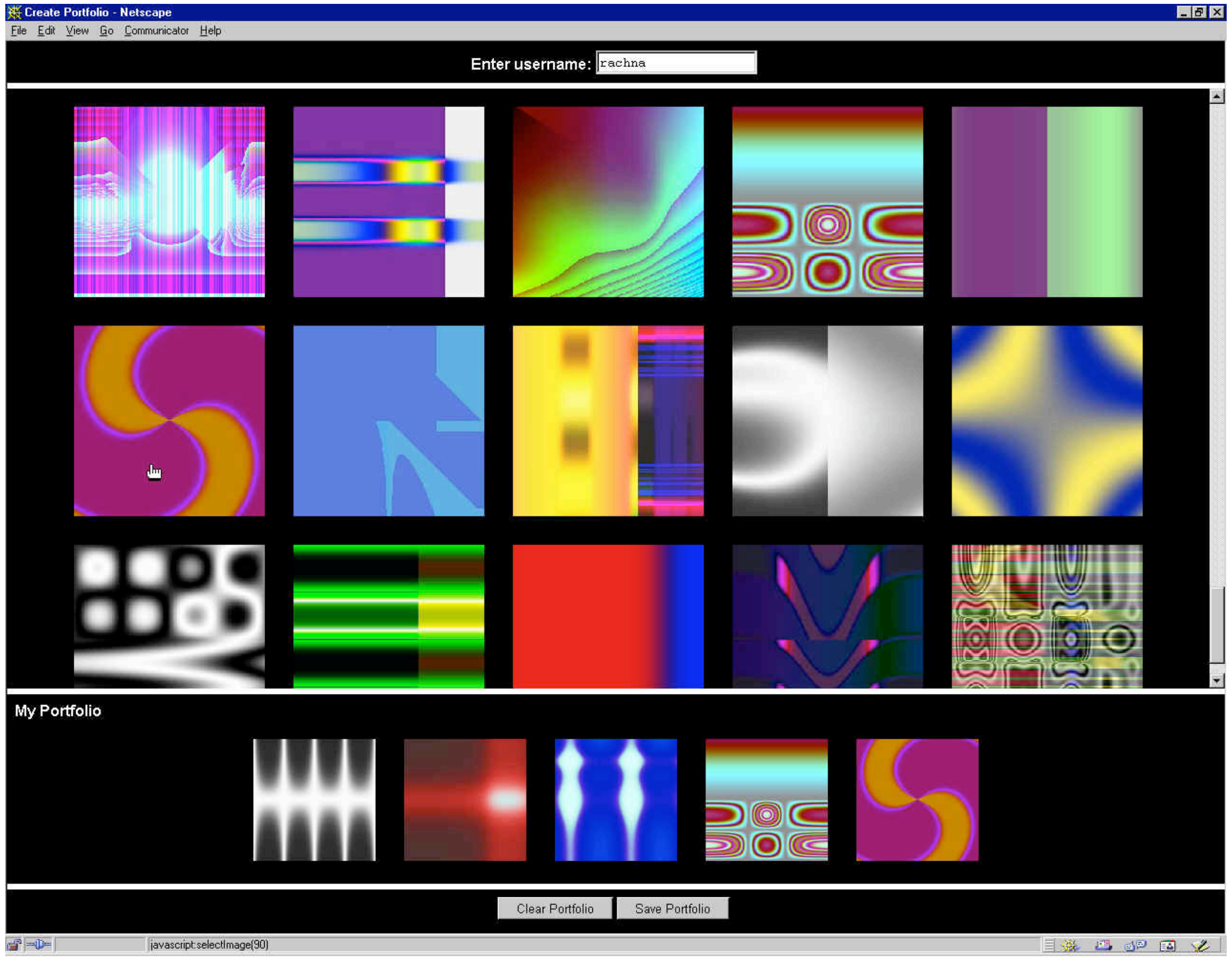
Select your images please

Passfaces
“select the face from your password set”



Deja Vu (Dhamija & Perrig, 2000)

“select the images from your password set”



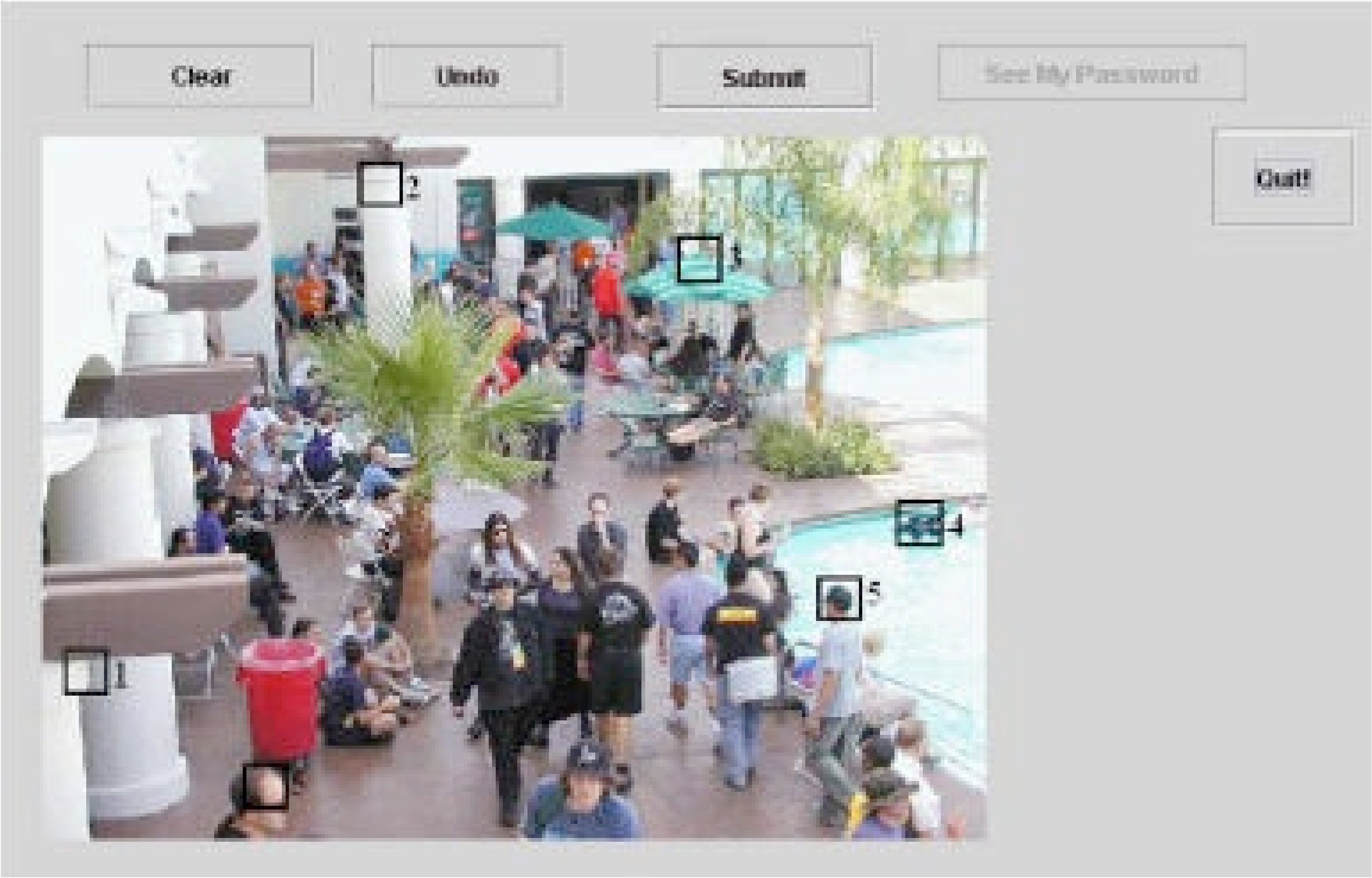
Create Portfolio - Netscape
File Edit View Go Communicator Help
My Portfolio
Clear Portfolio
Save Portfolio

Enter username: rachna

javascript:selectImage(90)

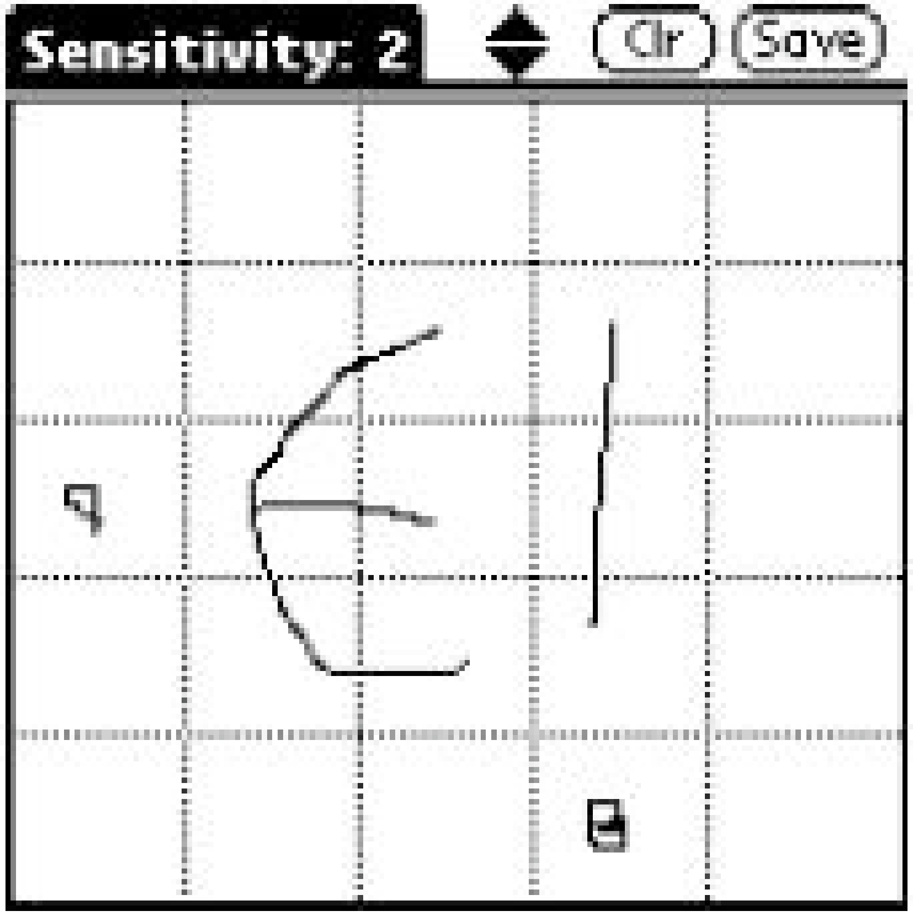
PassPoints (Wiedenbeck et al., 2005)

“click on the points in the image that constitute your password”

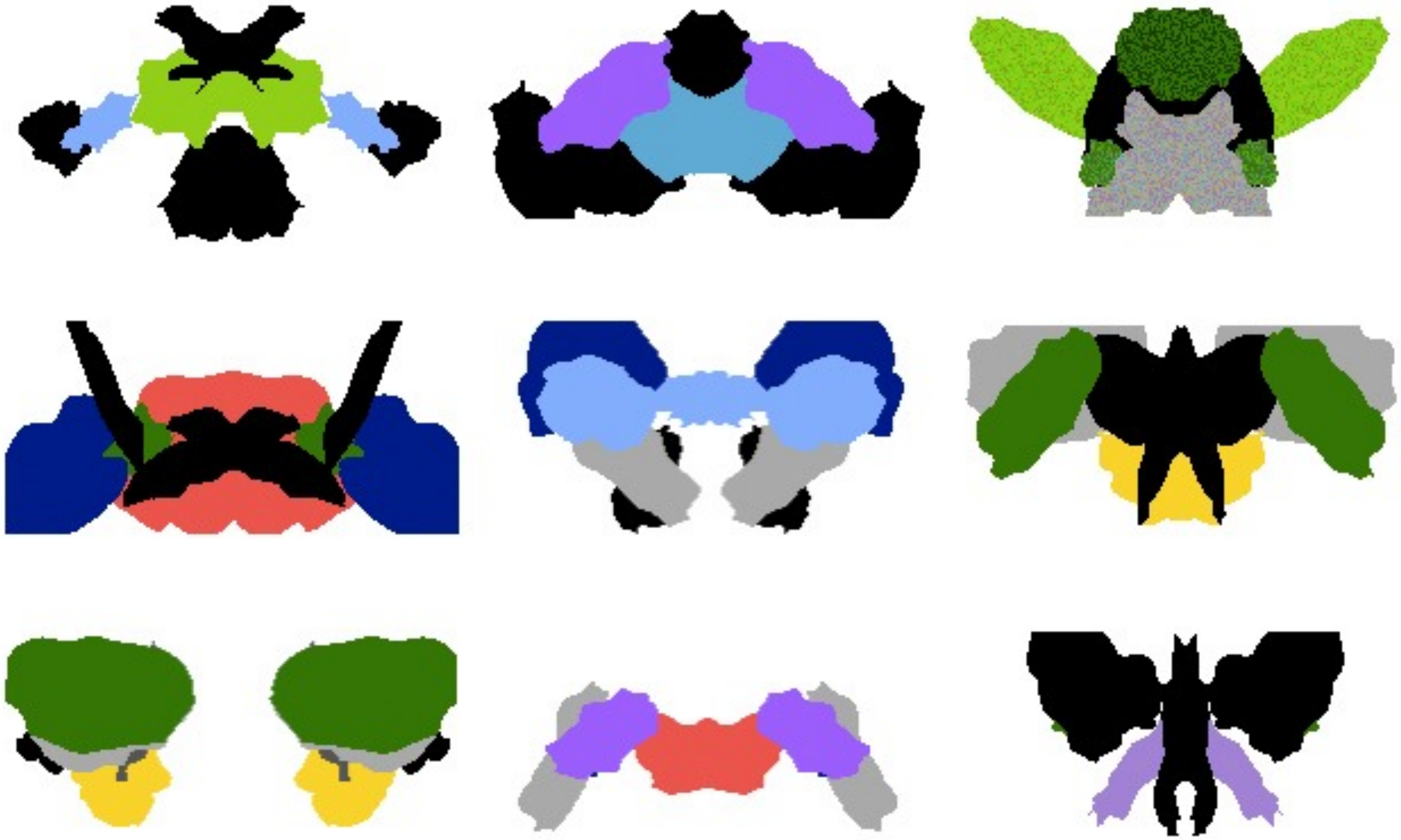


Draw-a-Secret: Gestural Authentication (Jermyn et at., 1999)

"recreate the drawing that you use as a password"



Stubblefield & Simons Inkblot Creatures (2004)



- Name each blob
- Determine the first and last letter of each name
- Concatenate the letters to form a password

http://research.microsoft.com/en-us/news/features/inkblots.aspx

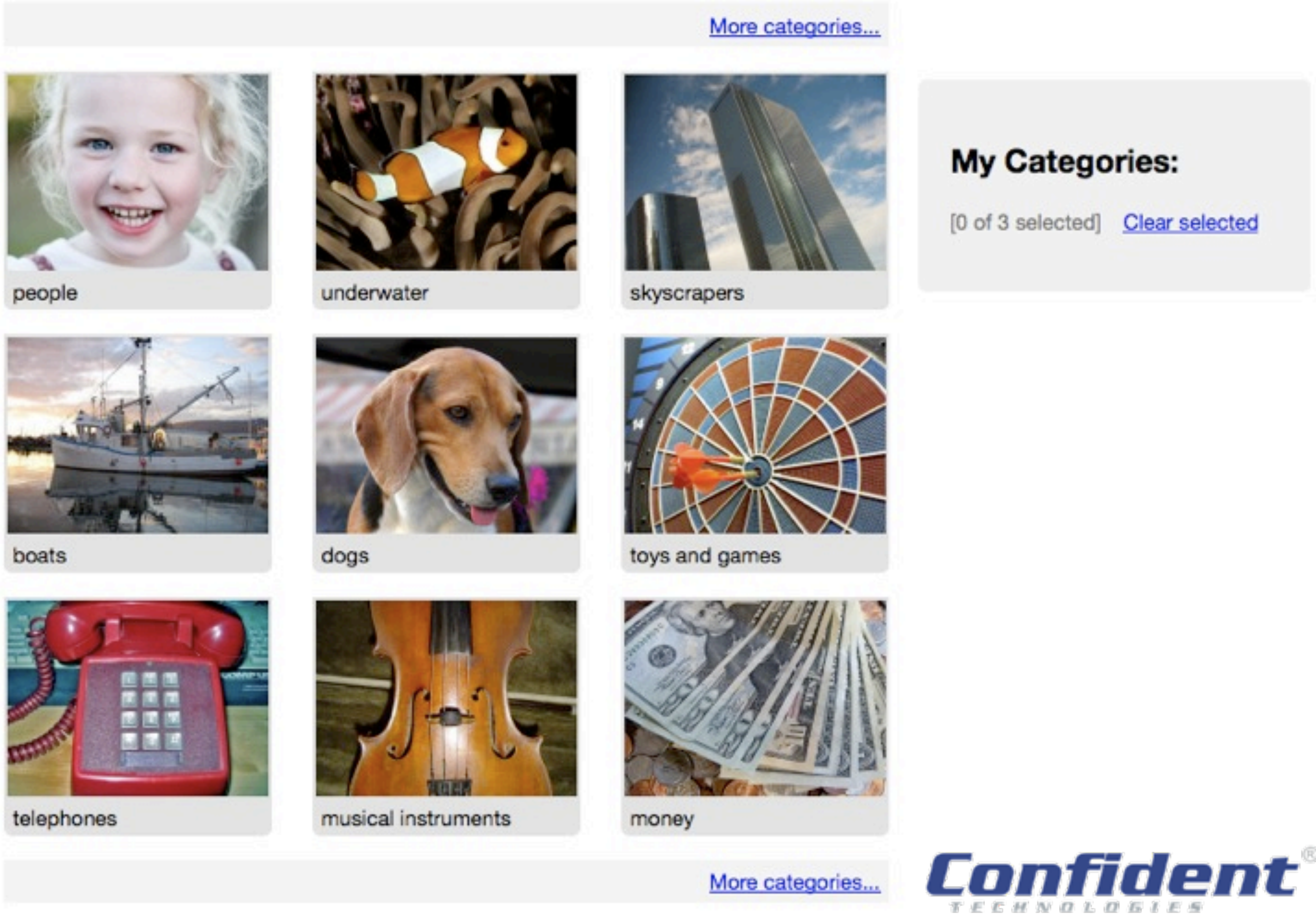
Image-based Authentication through ImageShield™

(formerly myVidoop)

- At **registration** the user selects categories of images
- At **authentication**, the user
  - is presented with a grid of randomly generated images
  - chooses the images that match their categories
  - enters the corresponding letter or number
- This creates a secure, one-time access code

Confident® TECHNOLOGIES

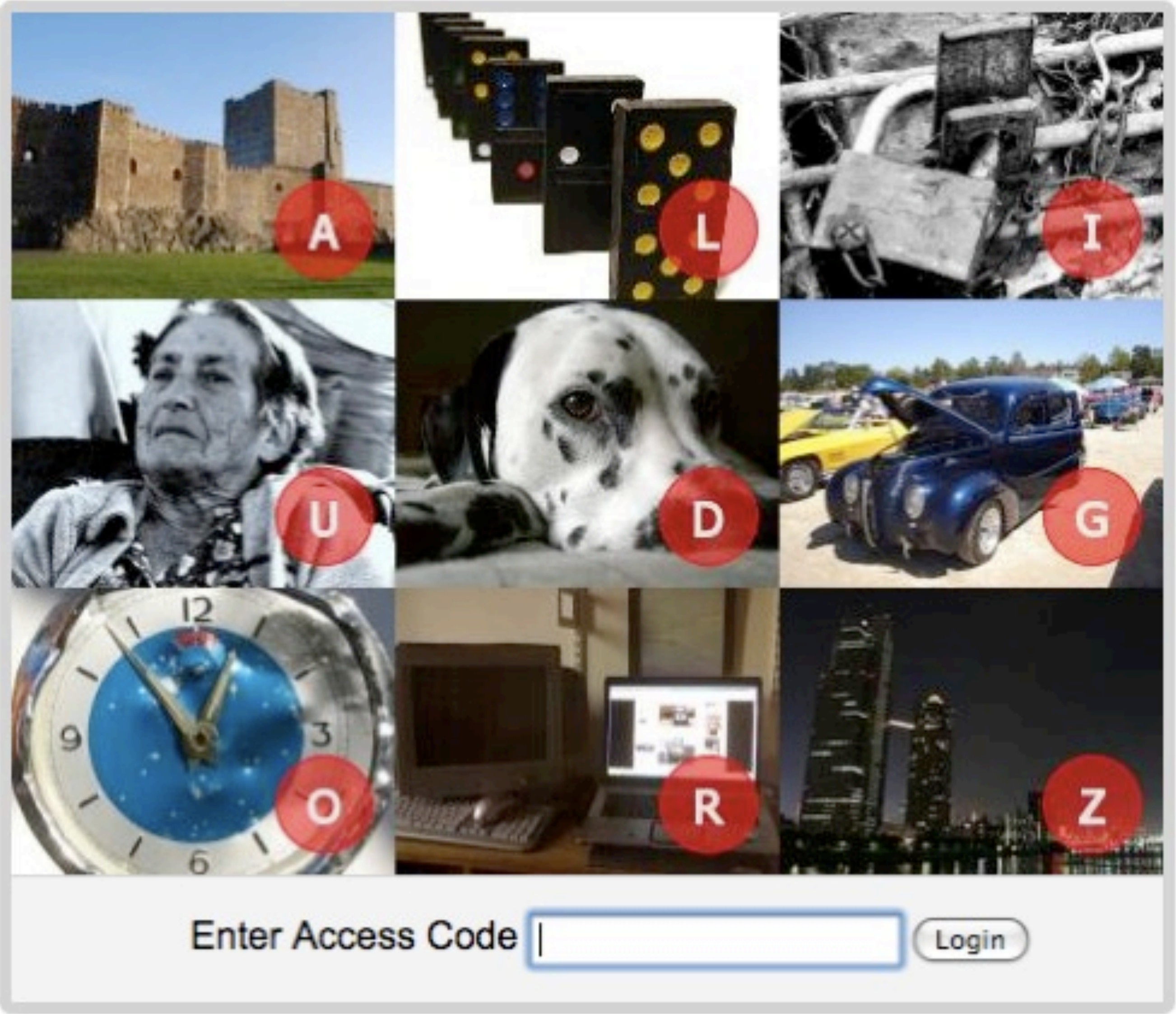
Category Selection at Registration



Confident® TECHNOLOGIES

University of Idaho
A LEGACY OF LEADING

Image Search for Authentication



Composite Scene Authentication (CSA)

Johnson and Werner (2006, 2007)

- **Composite Scenes as Passwords**
  - A scene combines *n* scene-elements into one picture
  - Scene elements are randomly selected, one from *n* different categories
  - Each scene-element needs to be selected out of *m* choices during authentication
  - Strength of password (bits) = $n * \log_2 (m)$
- **Authentication**
  - Sequence of n challenge screens
  - Each challenge screen is organized by category
  - User has to select 1 scene-element per screen

Composite Scene Authentication (CSA)

Johnson and Werner (2006, 2007)

- **Advantages of a Scene**
  - –Password elements are bound together by scene
  - –Each element carries multiple sources of information
    - multiple semantic characteristics
    - multiple visual characteristics
    - interaction with other elements within the scene
- this leads to **Redundancy**

Composite Scene Authentication (CSA)

Johnson and Werner (2006, 2007)

- **Advantages of categorical order during authentication**
  - Category cues the relevant scene element
  - Reduction of uncertainty in visual search
  - Visual search space more homogeneous
- **Recognition with additional cues**

Categories of Passcode Elements

female person

child

male person

food item

wild animal

cat or dog

inanimate object

musical instrument

environmental setting

each *password* consists of *9 elements*

female person child male person

food item wild animal cat or dog

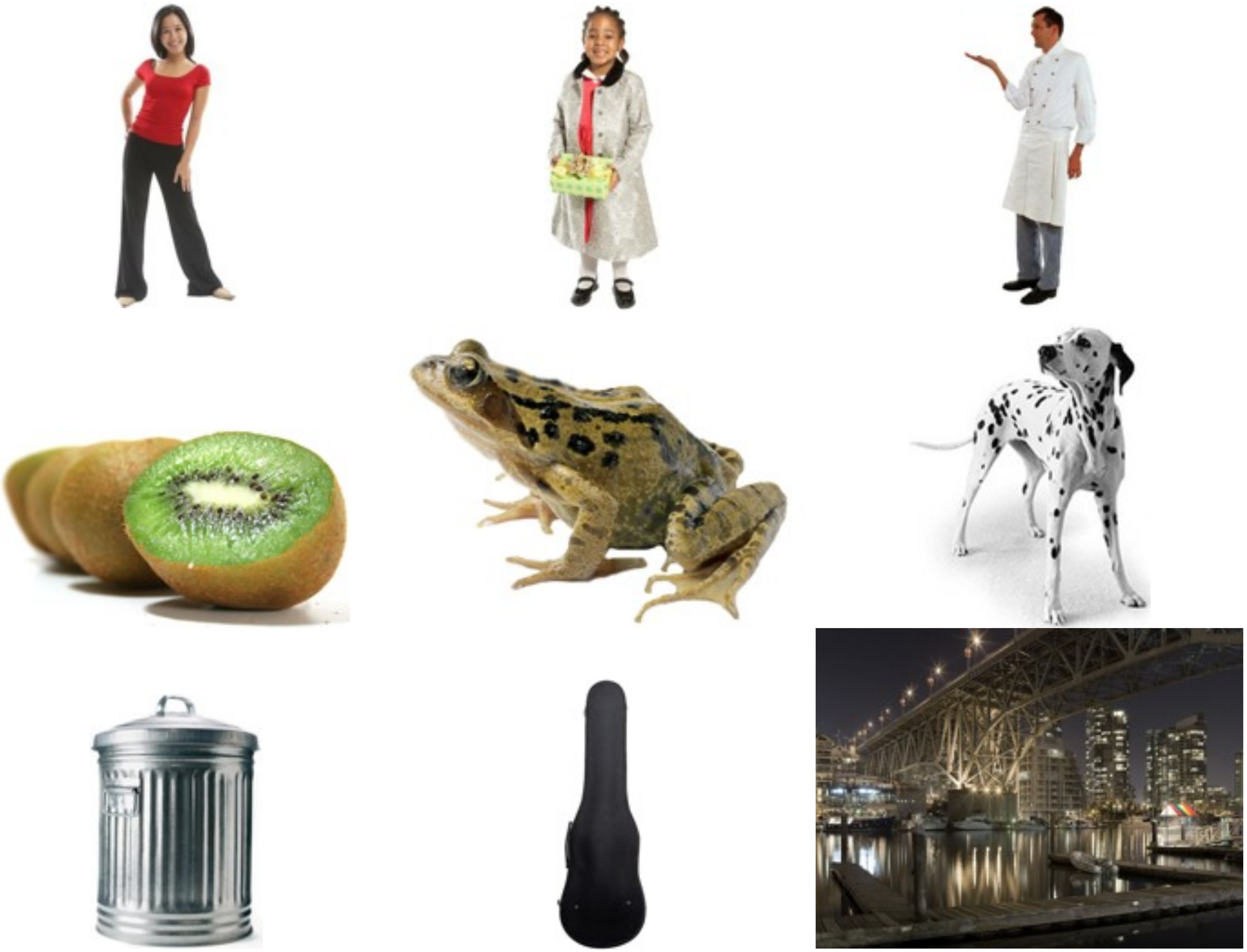
musical instrument

inanimate object environmental setting

each *password* consists of *9 elements*

female person	child	male person
food item	wild animal	cat or dog
inanimate object	musical instrument	setting

each *password* consists of *9 elements*



each *password* consists of 9 *elements*

one *character* of the *password*

1 bit

2 bit

3 bit

4 bit

5 bit

Empirical Studies

- **Comparative Evaluation**
  - How do grahical authentication systems fare?
  - CSA pitted against three other well-known graphical authentication systems
- **Graphical password interference**
  - What happens, if more than one graphical password have to be remembered?
  - Different vs. same image sets for passwords
- **Categorical structure of visual search**
  - Does categorical structure of authentication screens produce a benefit for recognition performance?

Comparative Evaluation of Composite Scene Authentication (CSA)

- **3 variations of CSA**
  - **CSA composite**
  - **CSA serial**
  - **CSA serial + composite**
- **3 alternative graphical authentication systems**
  - **Spatial** (Blonder, 1996, Wiedenbeck, 2005)
  - **Tiled** (VIP, De Angeli et al. 2005)
  - **Facial** (Passfaces™, n.d.)
- Graphical and alphanumeric passwords of equal complexity

Comparative Evaluation of Composite Scene Authentication (CSA)

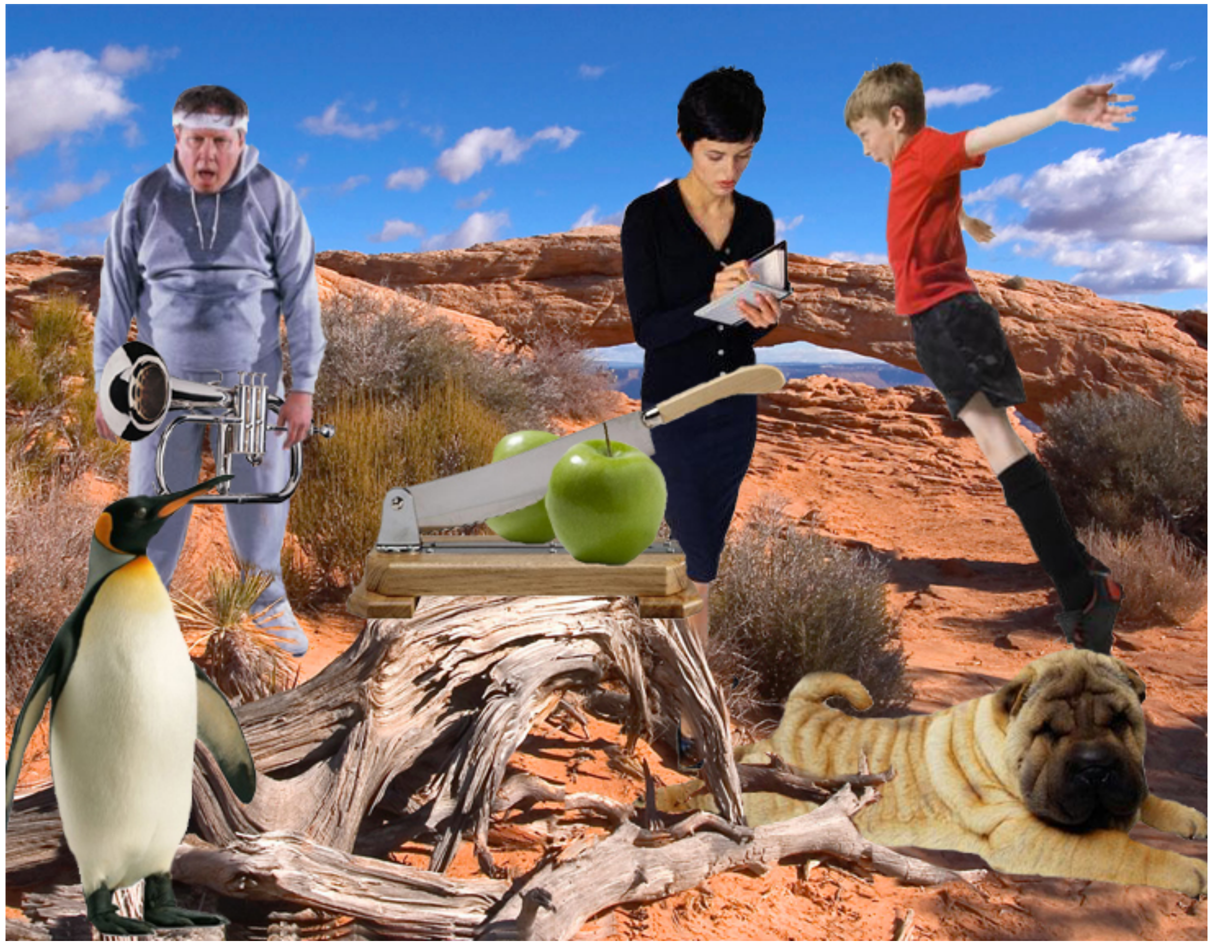
- **Variation of Strength of Passwords**
  - (36 or 46.5 bits)
- **Variation of Retention Interval**
  - (30 min, 1 week, 3 weeks)
- **Graphical passwords**
  - 36 bit = 15 distracters per authentication grid
  - 46.5 bit = 35 distracters per authentication grid
- **Alphanumeric passwords**
  - 36 bit: 9 char password randomly drawn from hexadecimal character space (n=16)
  - 46.5 bit: 9 char password randomly drawn from entire alphanumeric character space (n=36)

Comparative Evaluation of Composite Scene Authentication (CSA)

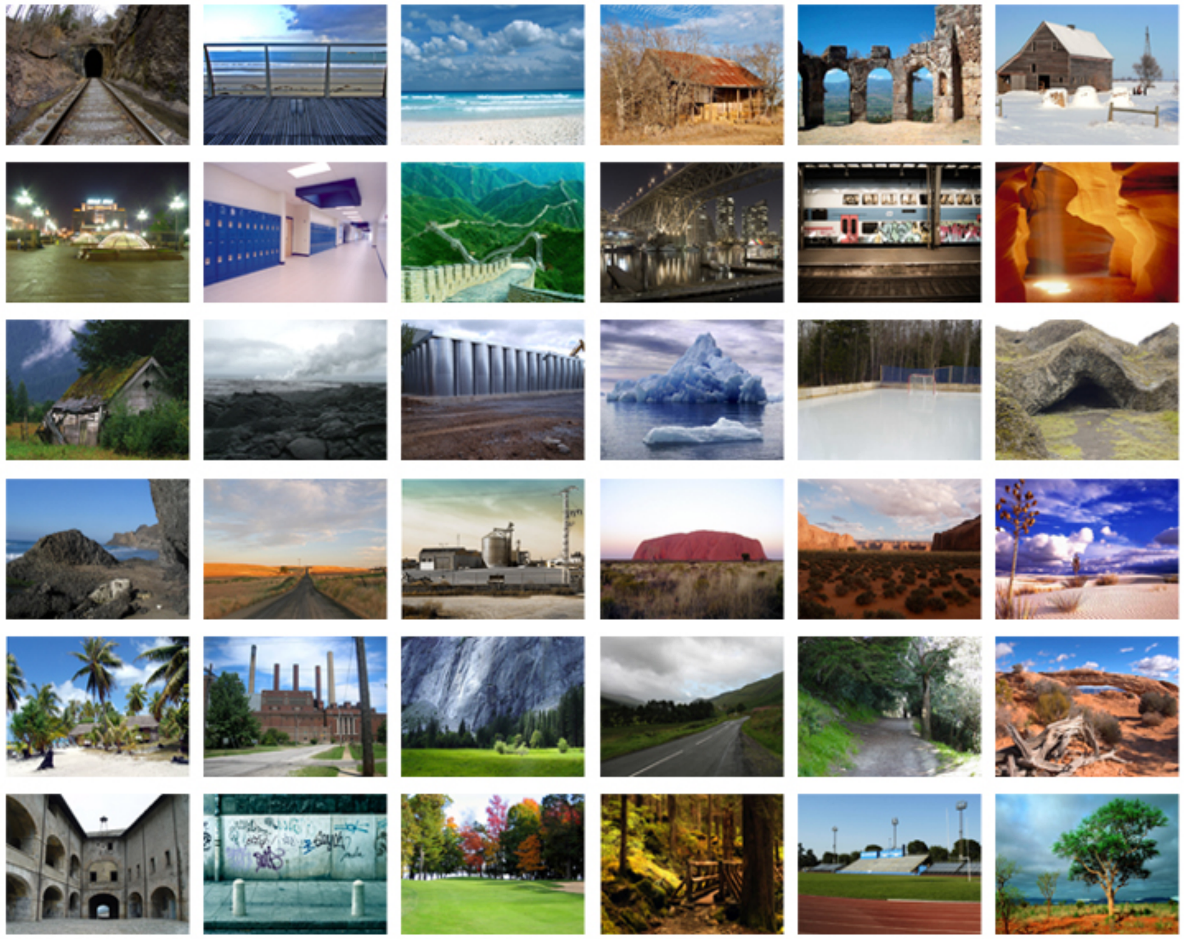
- **Graphical Materials**
  - – 324 images (36 in each category) for CSA and tiled groups
  - – 324 facial images for the facial passcode group
  - – 6 natural scenes for spatial passcode group
- **Graphical Passwords**
  - – 12 composite scenes for CSA composite
  - – 6 grids for tiled passcode group
- **Alphanumeric Materials**
  - – 24 alphanumeric character strings
  - – Virtual keyboard for password entry

CSA Composite

Password Image



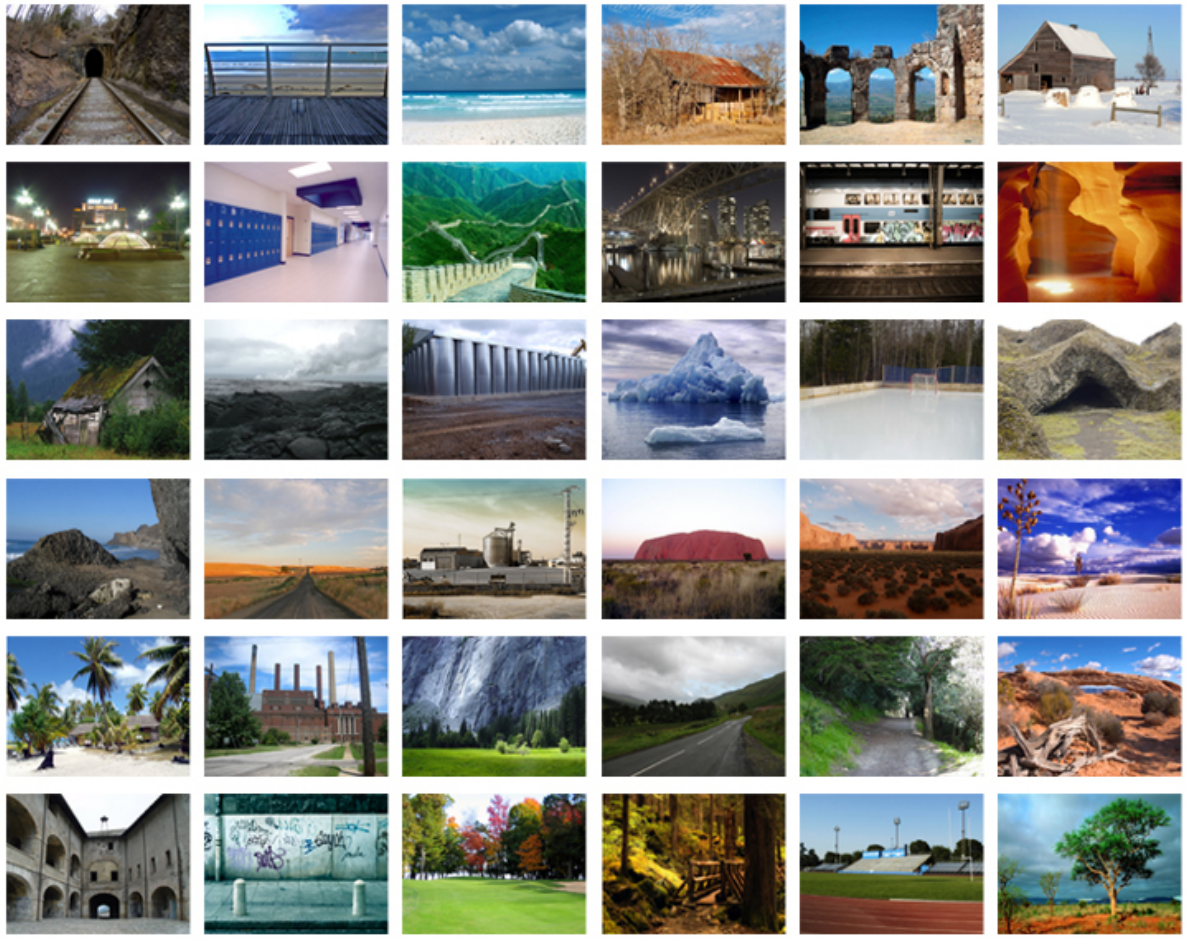
Authentication Challenges



CSA Serial

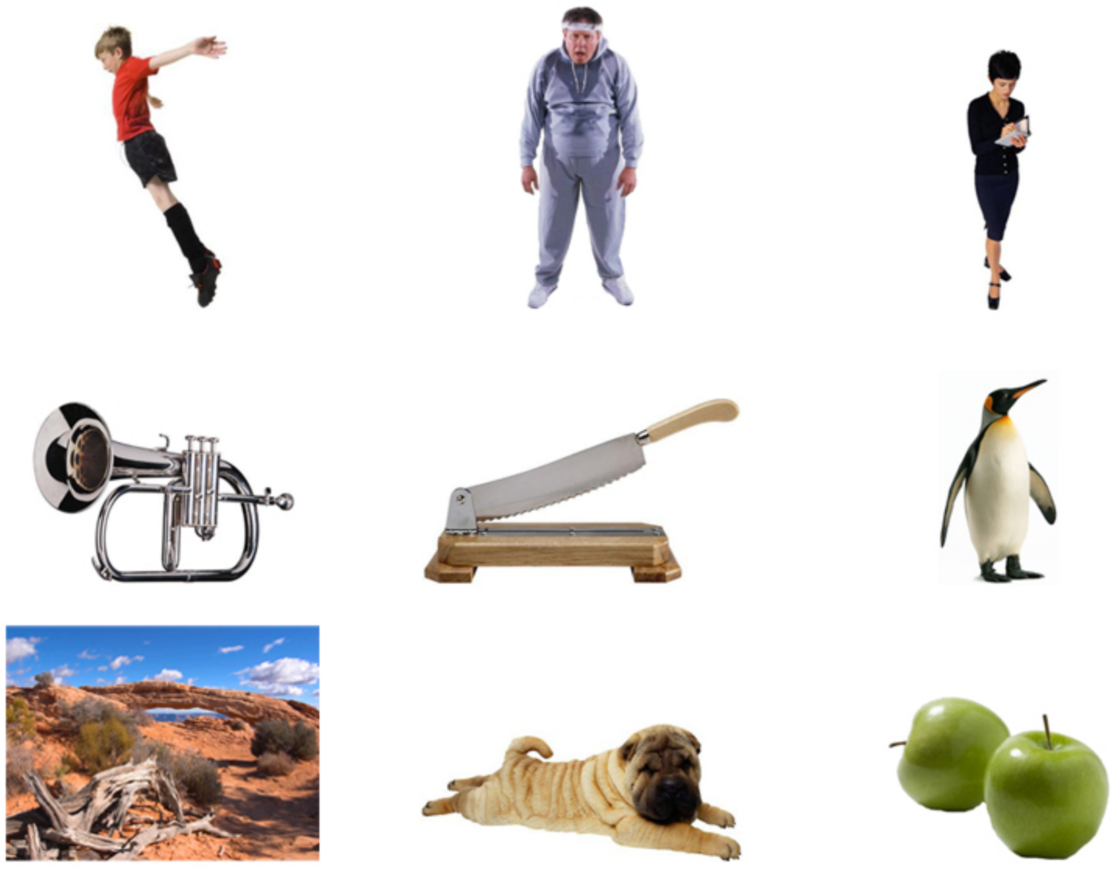
Password Elements

Authentication Challenges

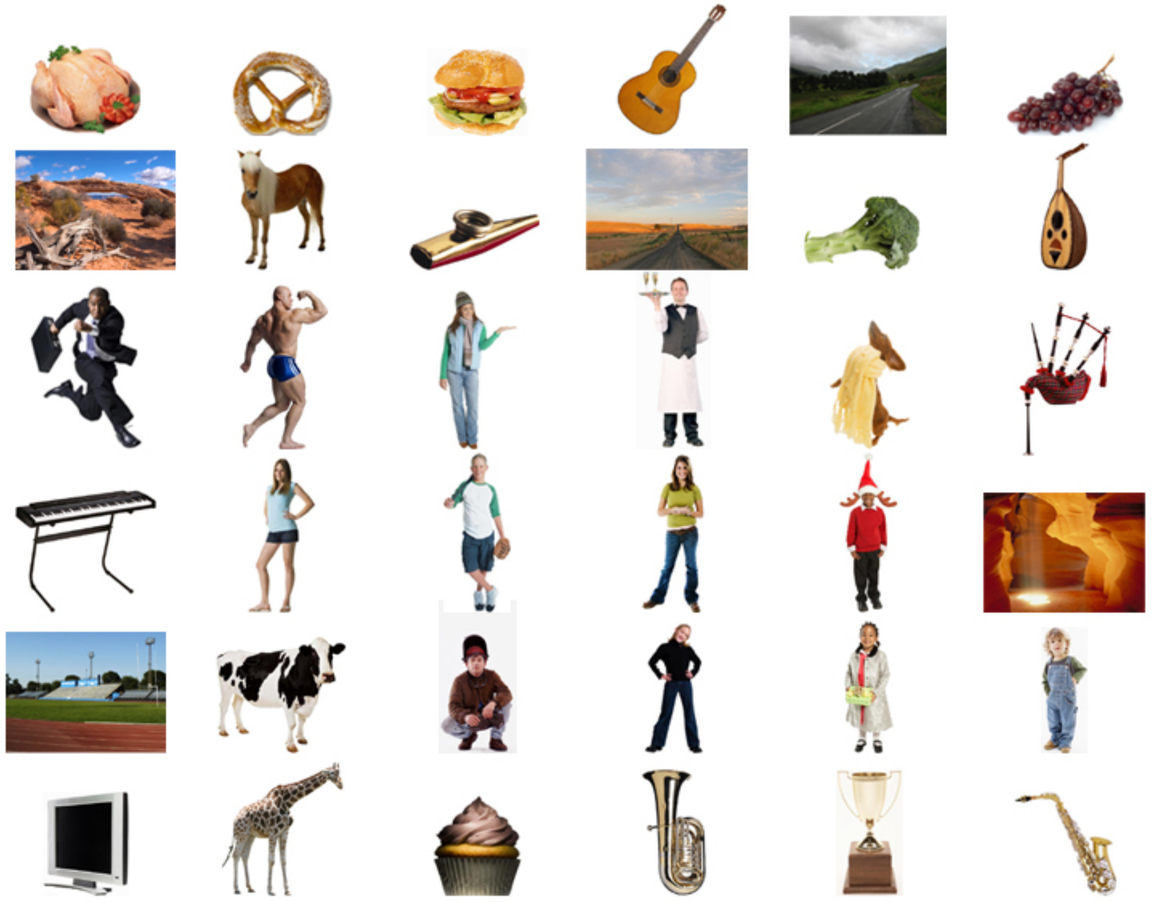


Tiled

Password Image



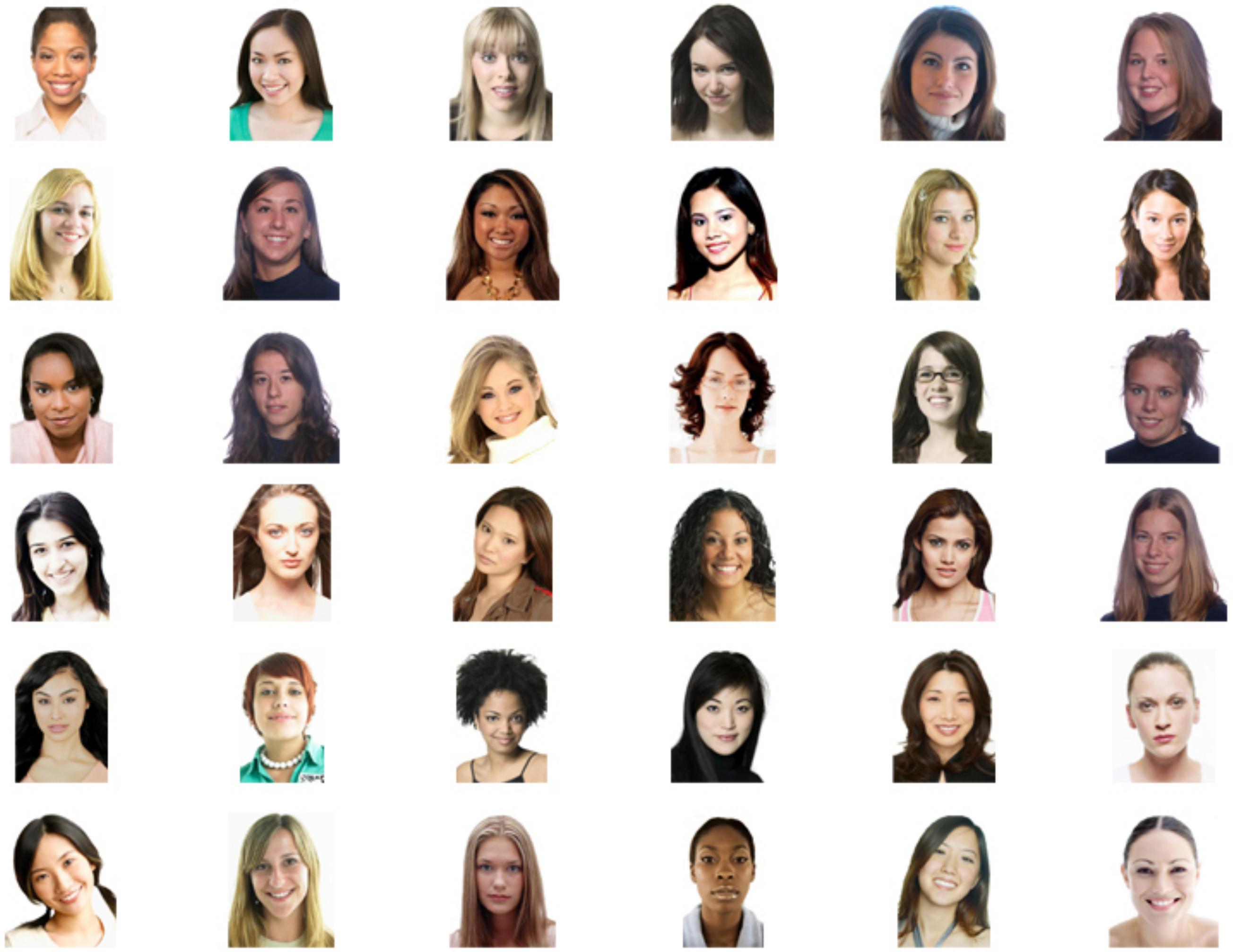
Authentication Challenges



Facial

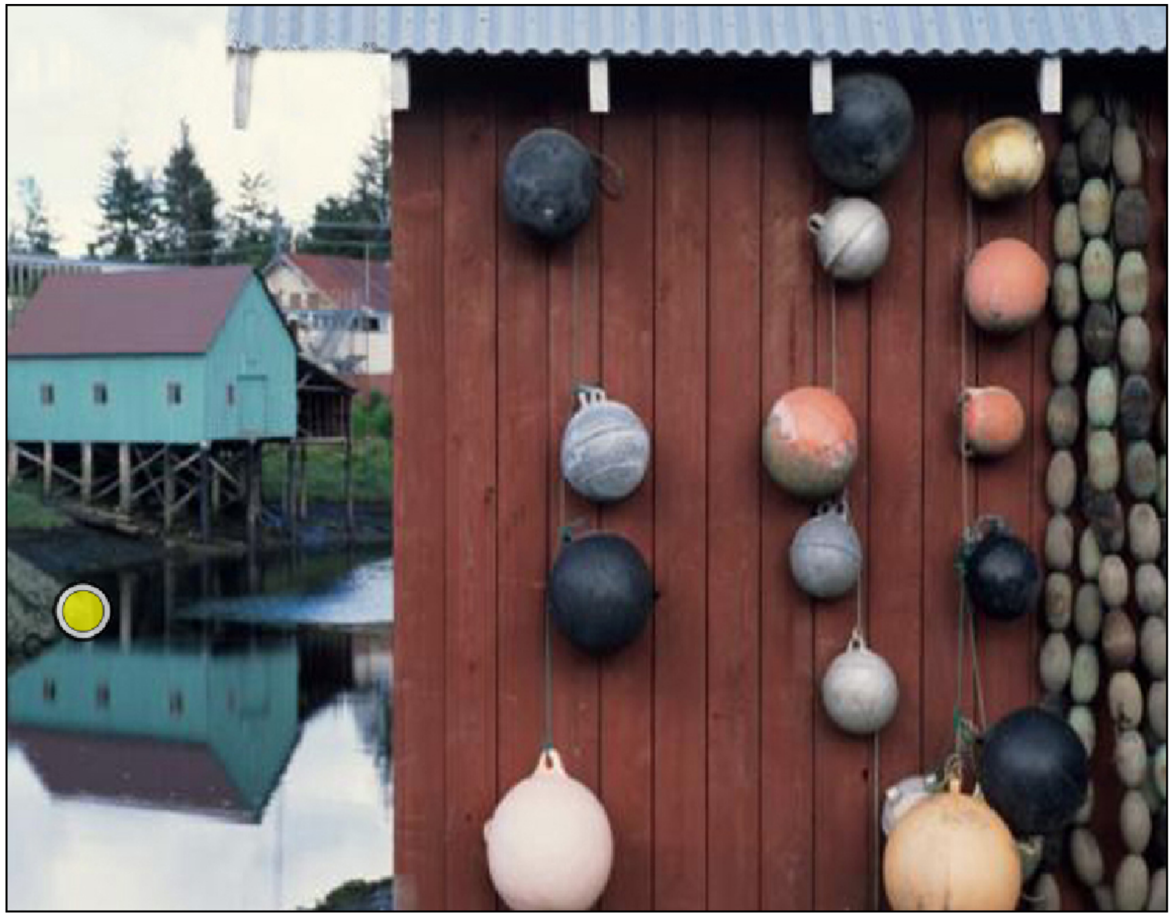
Password Image

Authentication Challenges

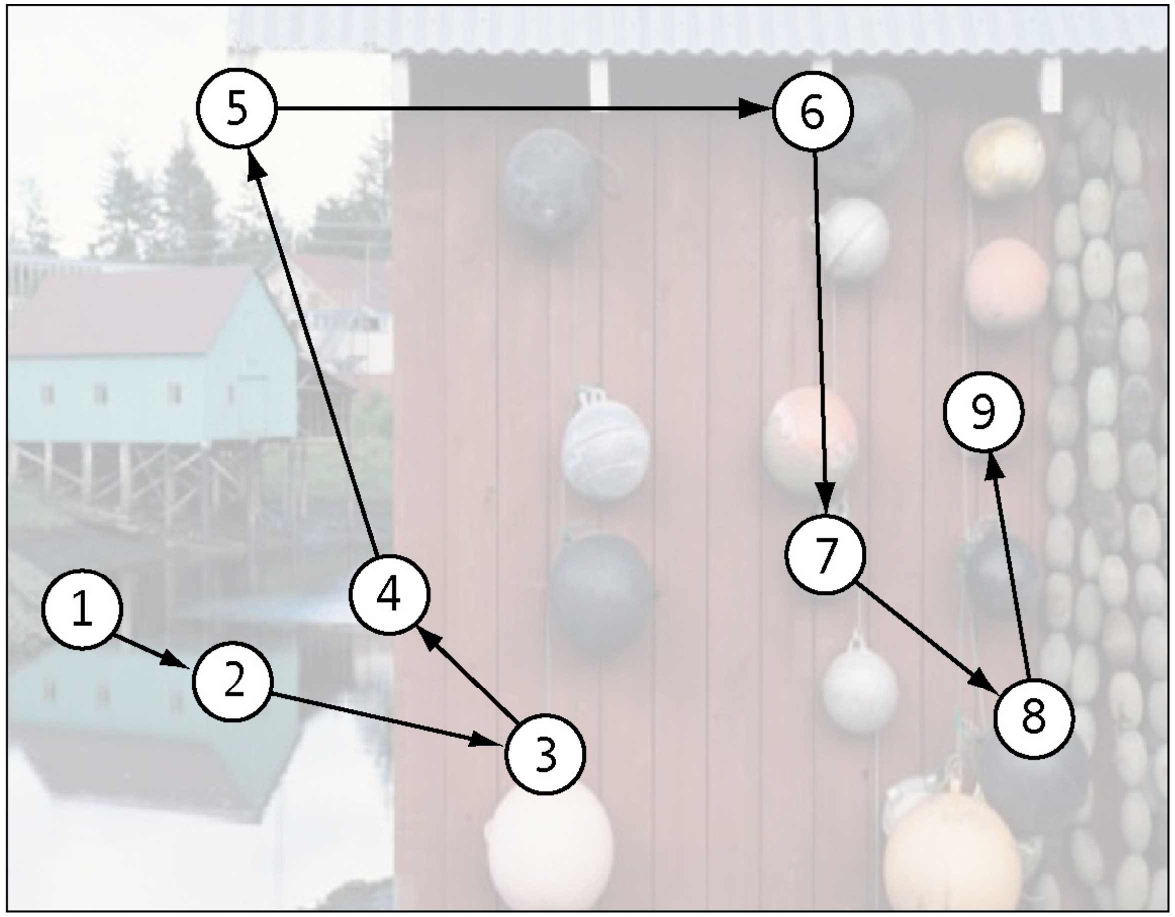


Spatial

Password Image

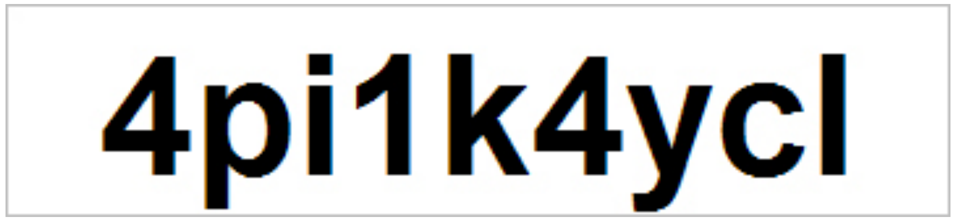


Authentication Challenges



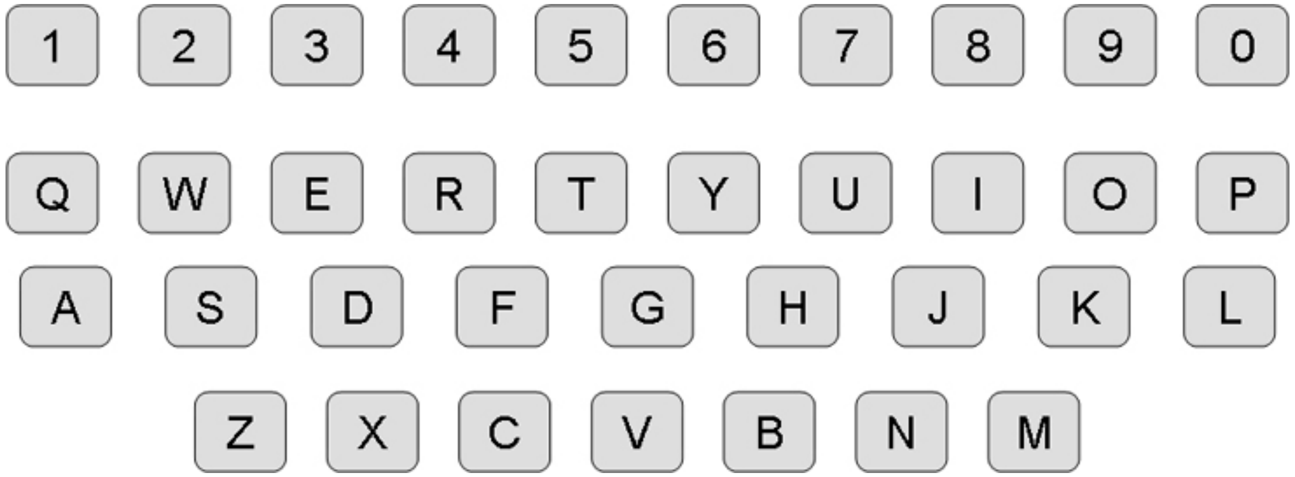
Alphanumeric Password

Password



4pi1k4ycl

Authentication Challenges



Comparative Evaluation of Composite Scene Authentication (CSA)

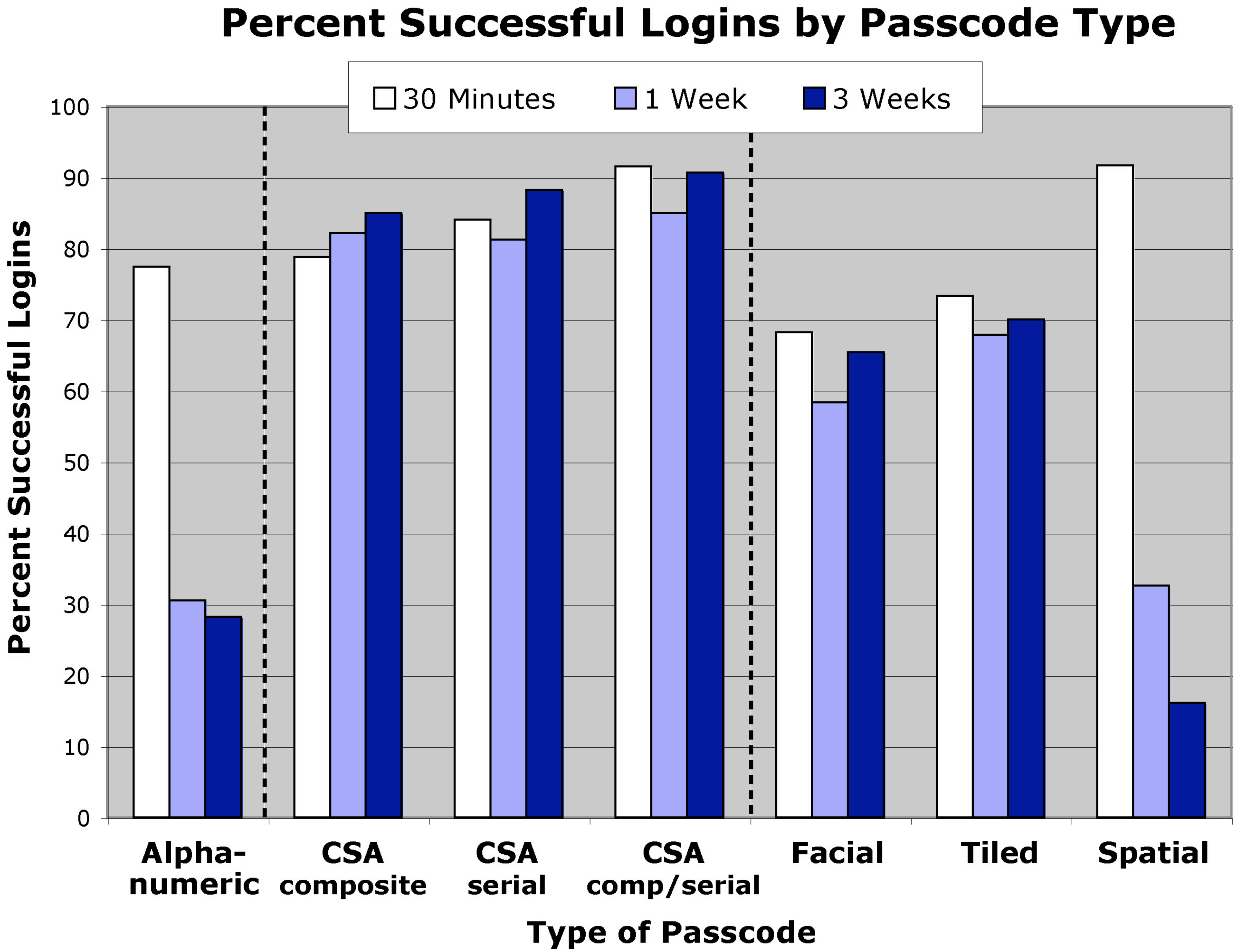
- **Encoding and 1st test phase**
  - General instruction, demographics, informed consent
  - Presentation of alphanumeric and graphical passcodes (either 36 or 46.5 bits)
  - Short story (30 minute presentation)
  - Recall / recognition test of memory for alphanumeric, graphical, and story information
  - Story test was independent measure of participants' memory and served as exclusion criterion

- **2nd and 3rd test phase**
  - Recall / recognition test only

Comparative Evaluation of Composite Scene Authentication (CSA)

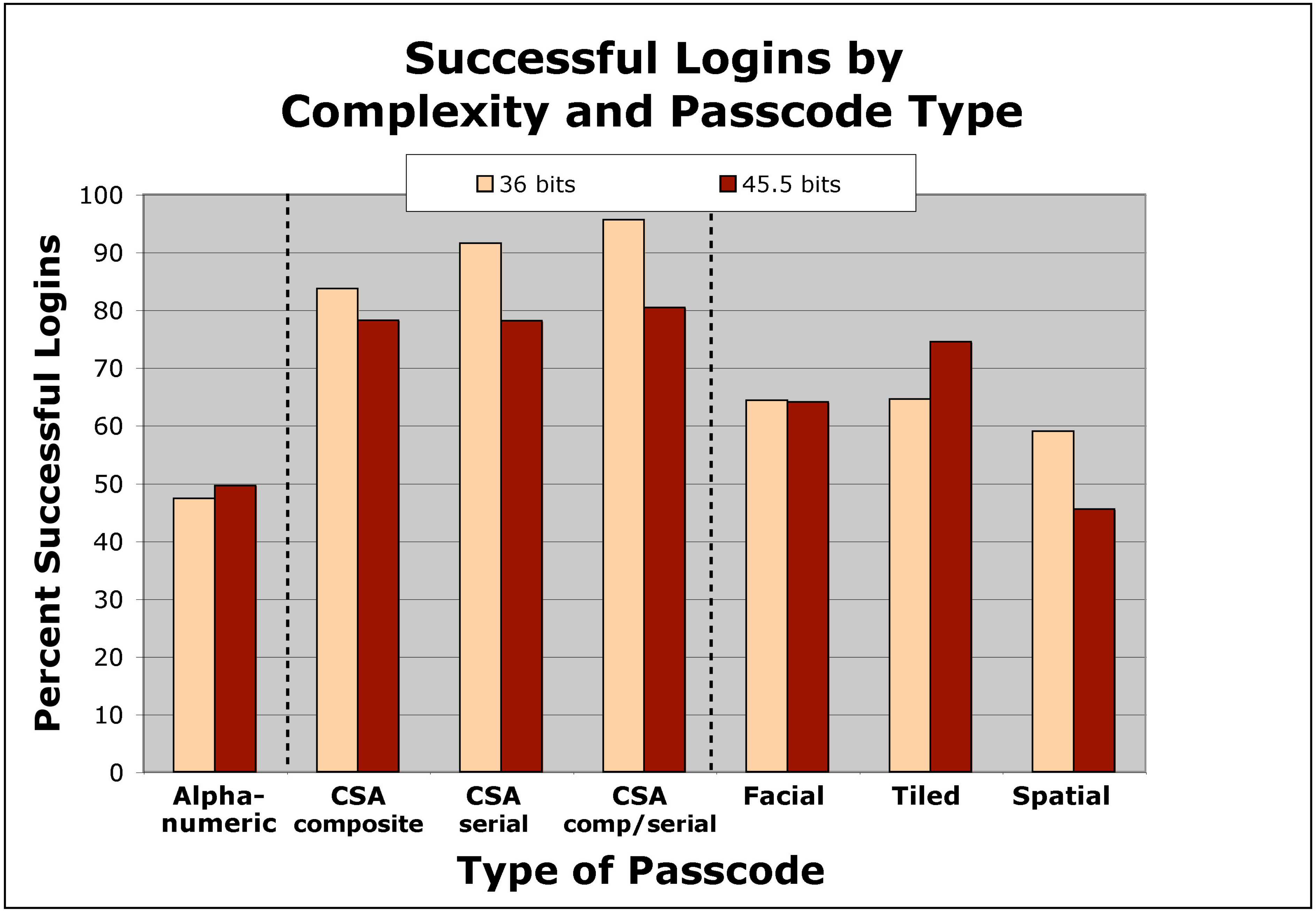
- **Total number of initial participants = 331**
  - 79 participants excluded because they either did not produce any data or because they failed a manipulation check (memory test on separate material)
  - 252 valid participants, 170 females (Mean Age = 24)
  - Participants compensated with extra course credit or a chance to win one of two cash prizes
  - Total #of participants for each retention interval:
    t_1: 252, t_2: 223, t_3: 163
- **Random assignment to one of 6 passcode groups**
- **Complexity randomly assigned within groups**

Comparative Evaluation of Composite Scene Authentication (CSA)



University of Idaho
A LEGACY OF LEADING

Comparative Evaluation of Composite Scene Authentication (CSA)



University of Idaho
A LEGACY OF LEADING

Composite Scene Authentication works best!

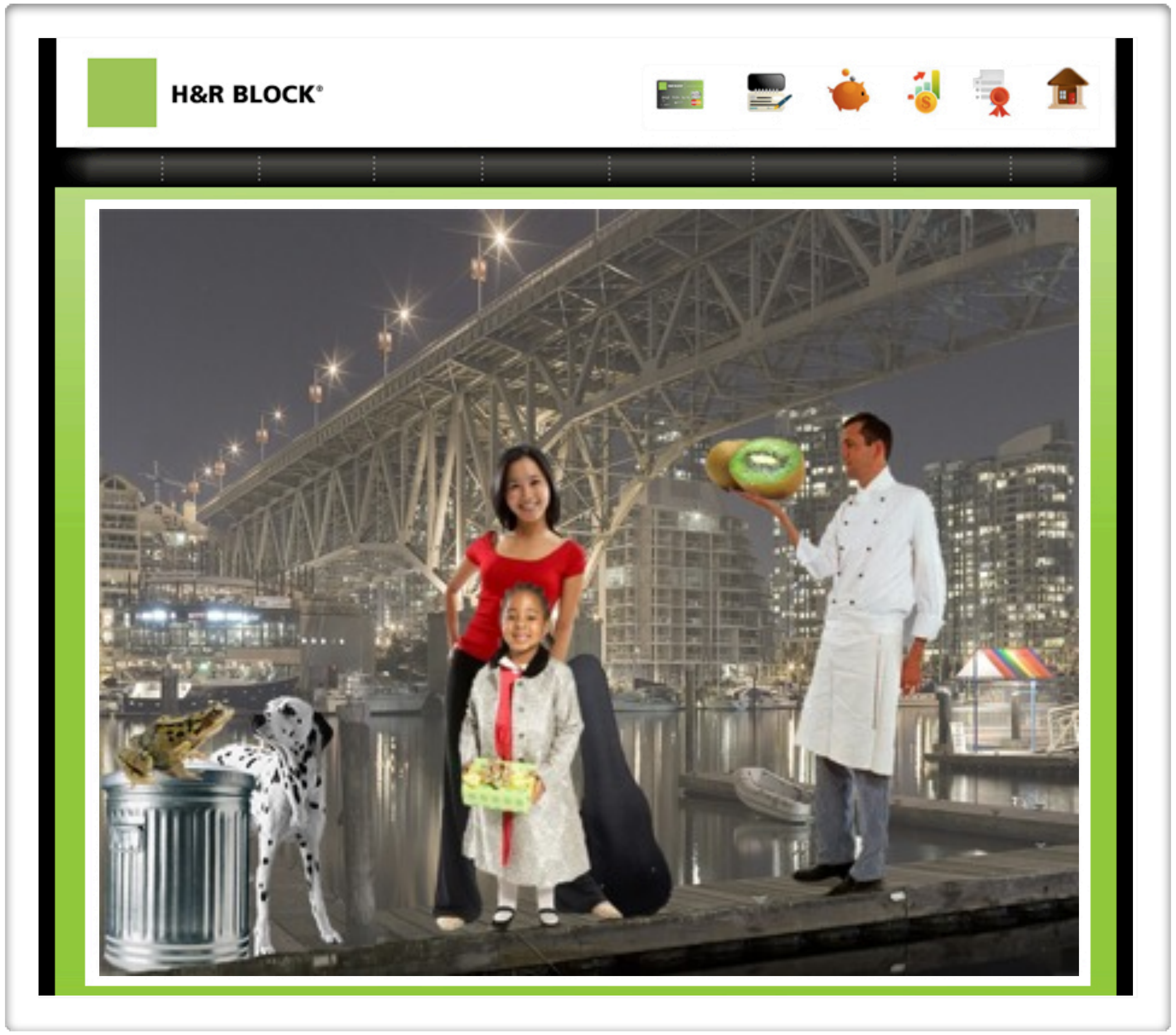
(spatial / locimetric systems are deficient)

Password Interference and Composite Scene Authentication (CSA)

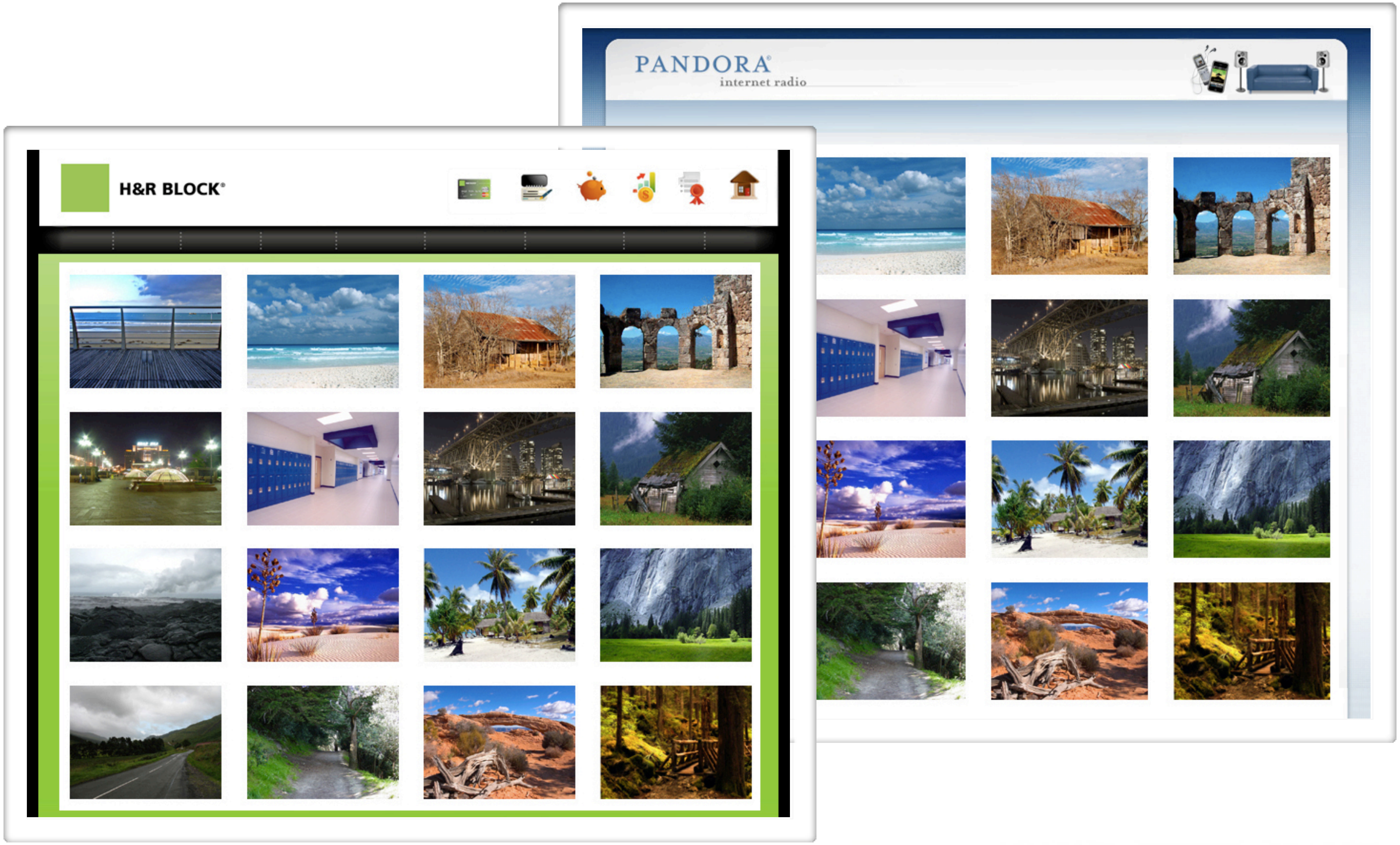
constant password strength = 36 bit

- **2 variations of CSA**
  - CSA composite
  - CSA serial + composite
- **2 alternative graphical authentication systems**
  - Tiled (VIP, De Angeli et al. 2005)
  - Facial (Passfaces™, n.d.)
- **2 Passwords (same type) to remember**
  - disambiguated through visual/semantic context
- **Same vs. different set of images for authenticating with graphical passwords**

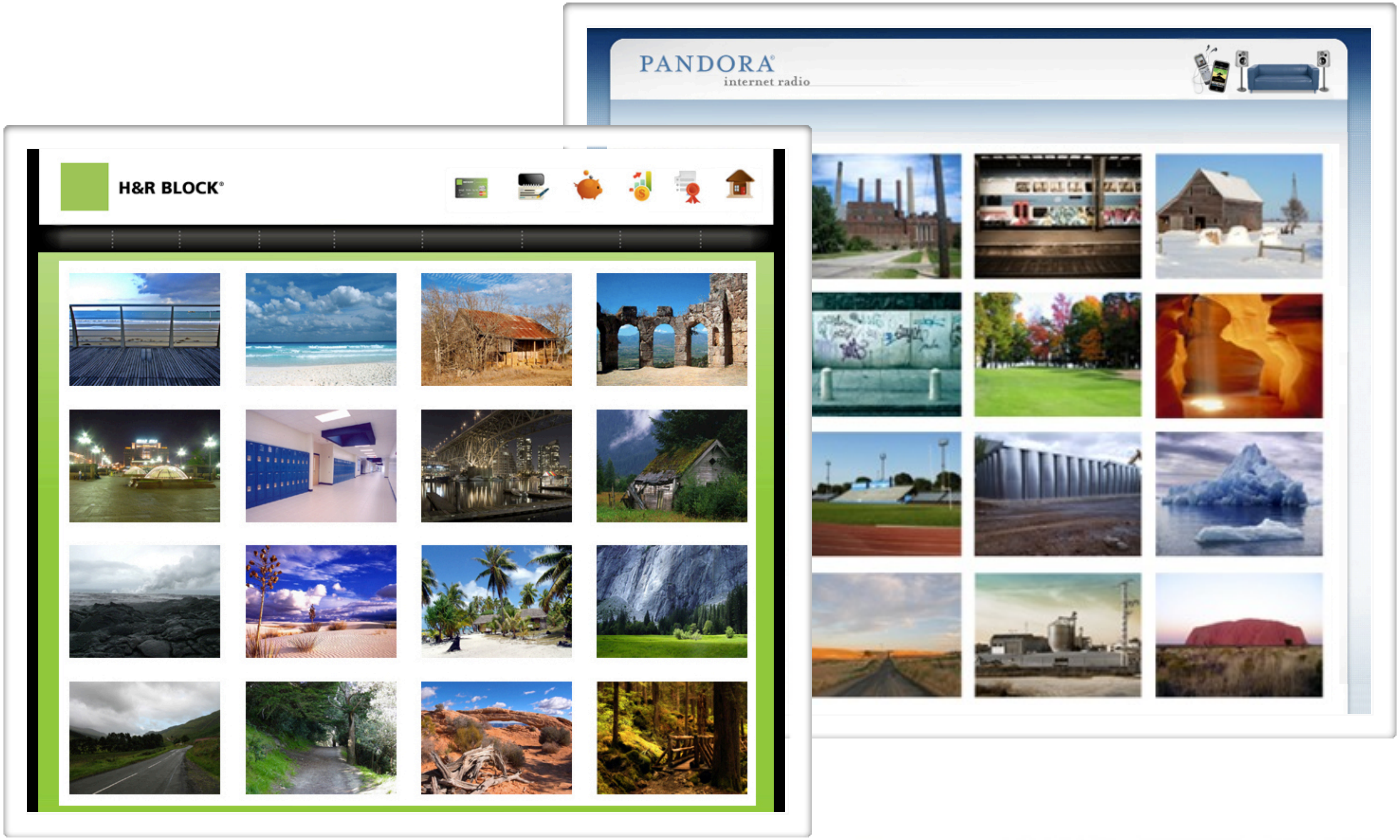
Password Interference and Composite Scene Authentication (CSA)



Password Interference:
Two Different Contexts - Same Image Set



Password Interference:
Two Different Contexts - Different Image Set



Password Interference and Composite Scene Authentication (CSA)

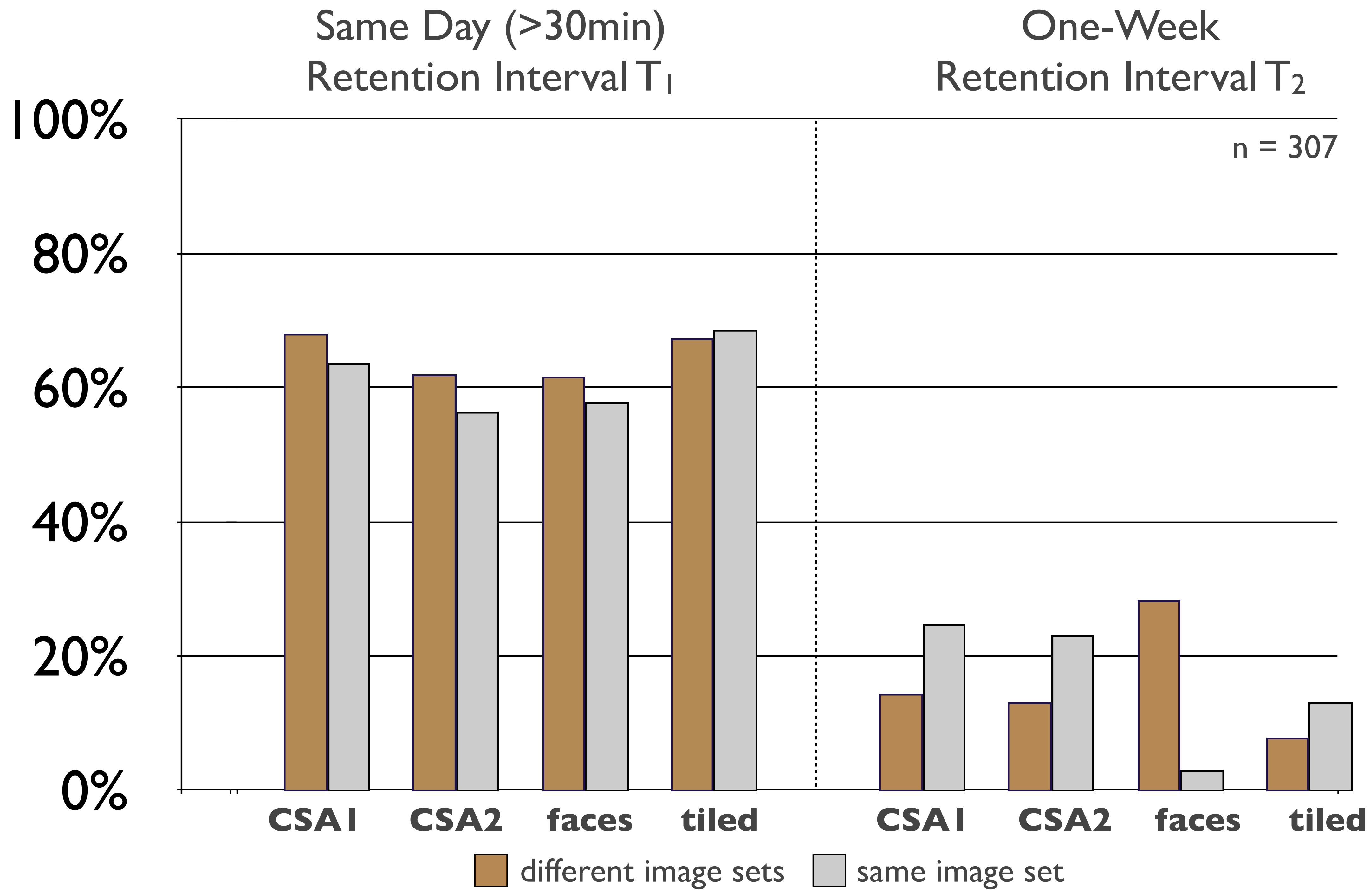
constant password strength = 36 bit

- **Total number of initial participants = 387**
  - 39 participants excluded because they failed a manipulation check (memory test on separate material)
  - 348 valid participants for T_1
  - 307 valid participants for T_1 & T_2
  - 174 valid participants for T_1, T_2, & T_3
  - Participants compensated with extra course credit
- **Random assignment to one of 4 passcode groups**
- **Same image set / different image set randomly assigned within group**

Password Interference and Composite Scene Authentication (CSA)

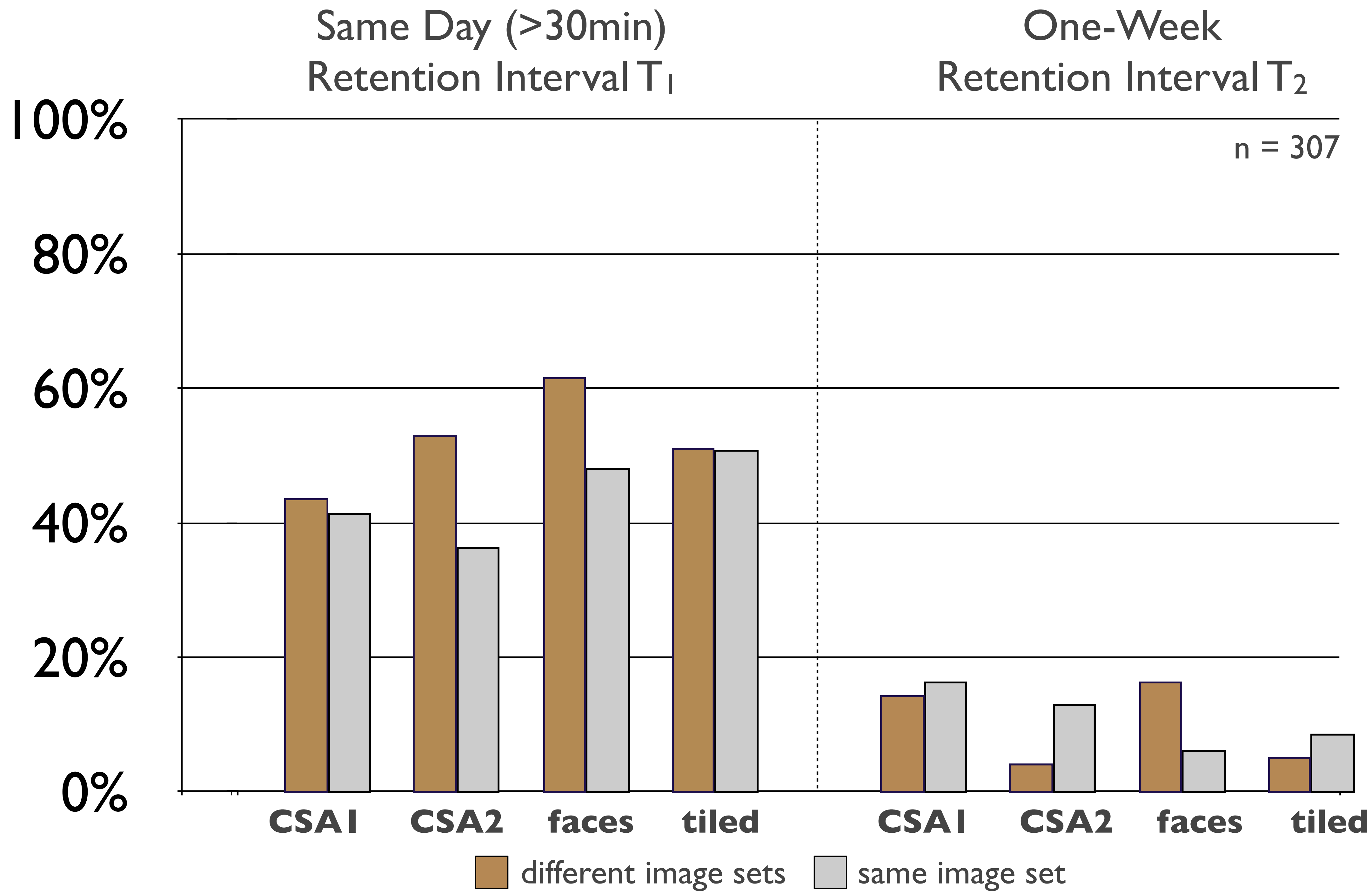
- **Encoding and 1st test phase**
  - General instruction, demographics, informed consent
  - Presentation of 2 alphanumeric and 2 graphical passcodes
  - Graphical passcodes were always of the same type
  - Short story (30 minute presentation)
  - Recall / recognition test of memory for alphanumeric, graphical, and story information
  - Recall / recognition dependent on visual context (Pandora or Tax-site)
  - Story test was independent measure of participants' memory and served as exclusion criterion
- **2nd test phase**
  - Recall / recognition test only
  - Recall / recognition again dependent on visual context (Pandora or Tax-site)

Authentication Success for *First* Alphanum Password

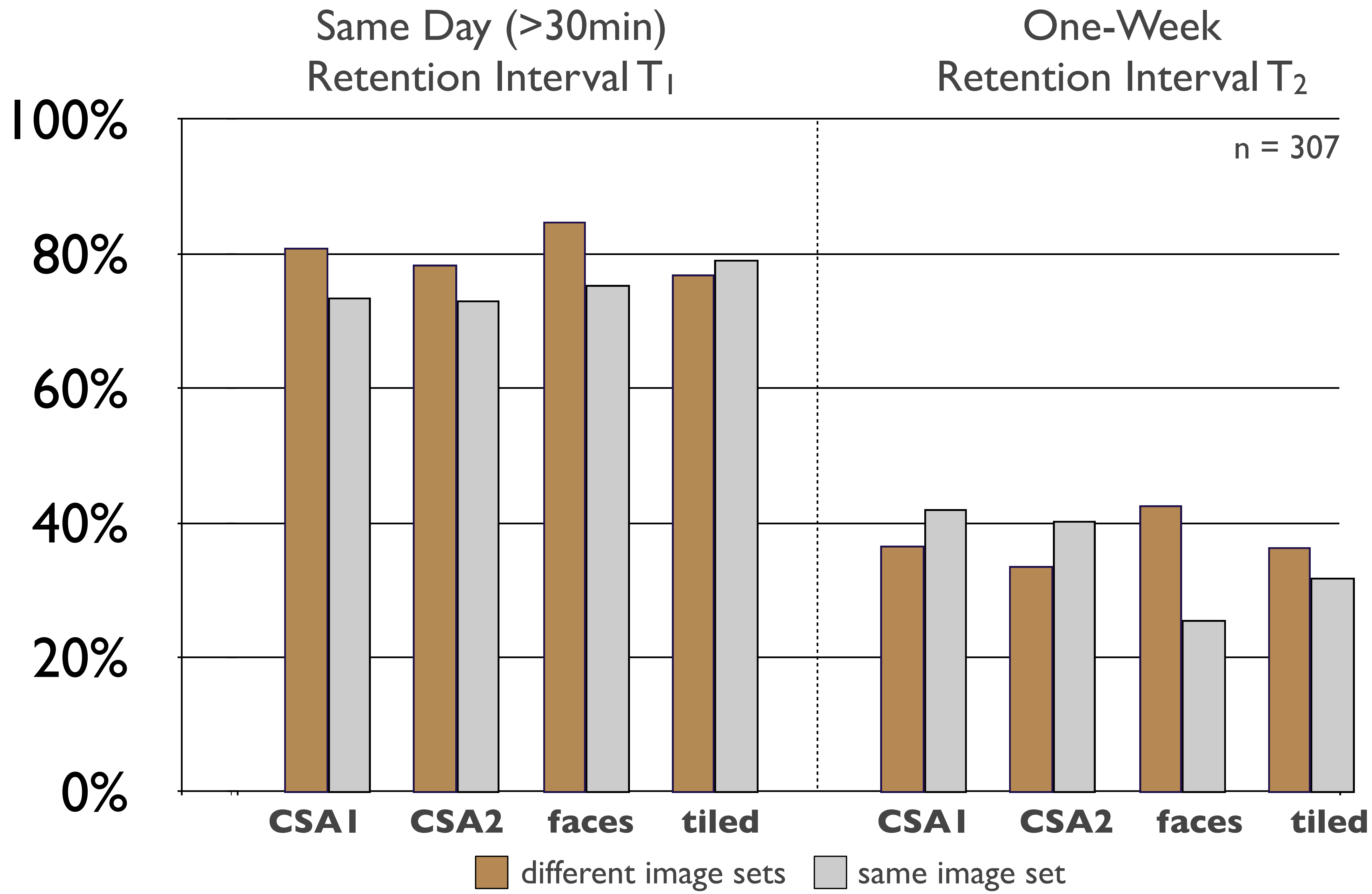


University of Idaho
A LEGACY OF LEADING

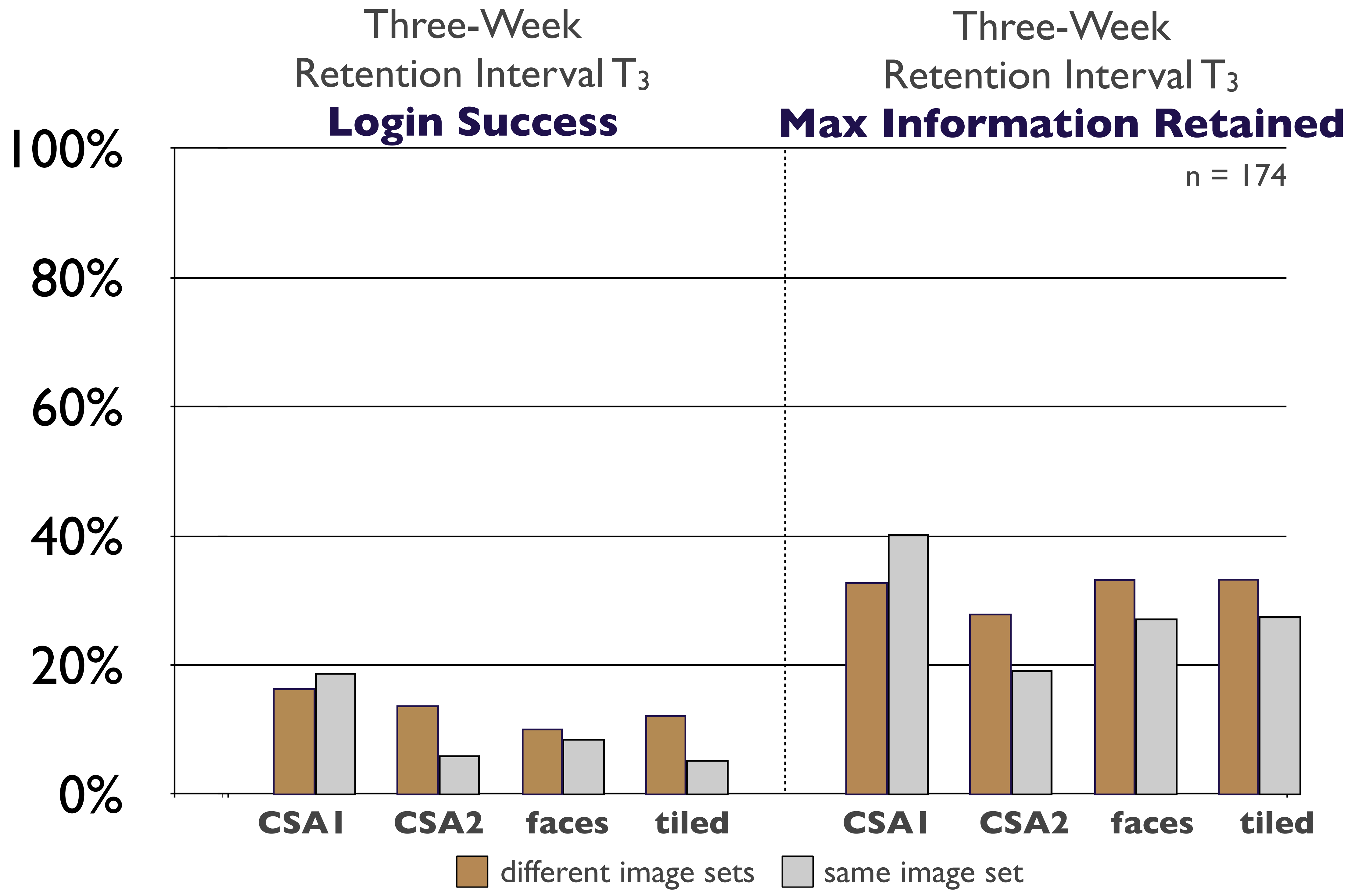
Authentication Success for *Second* Alphanum Password



Max Information Retained (Both Alphanum Passwords)

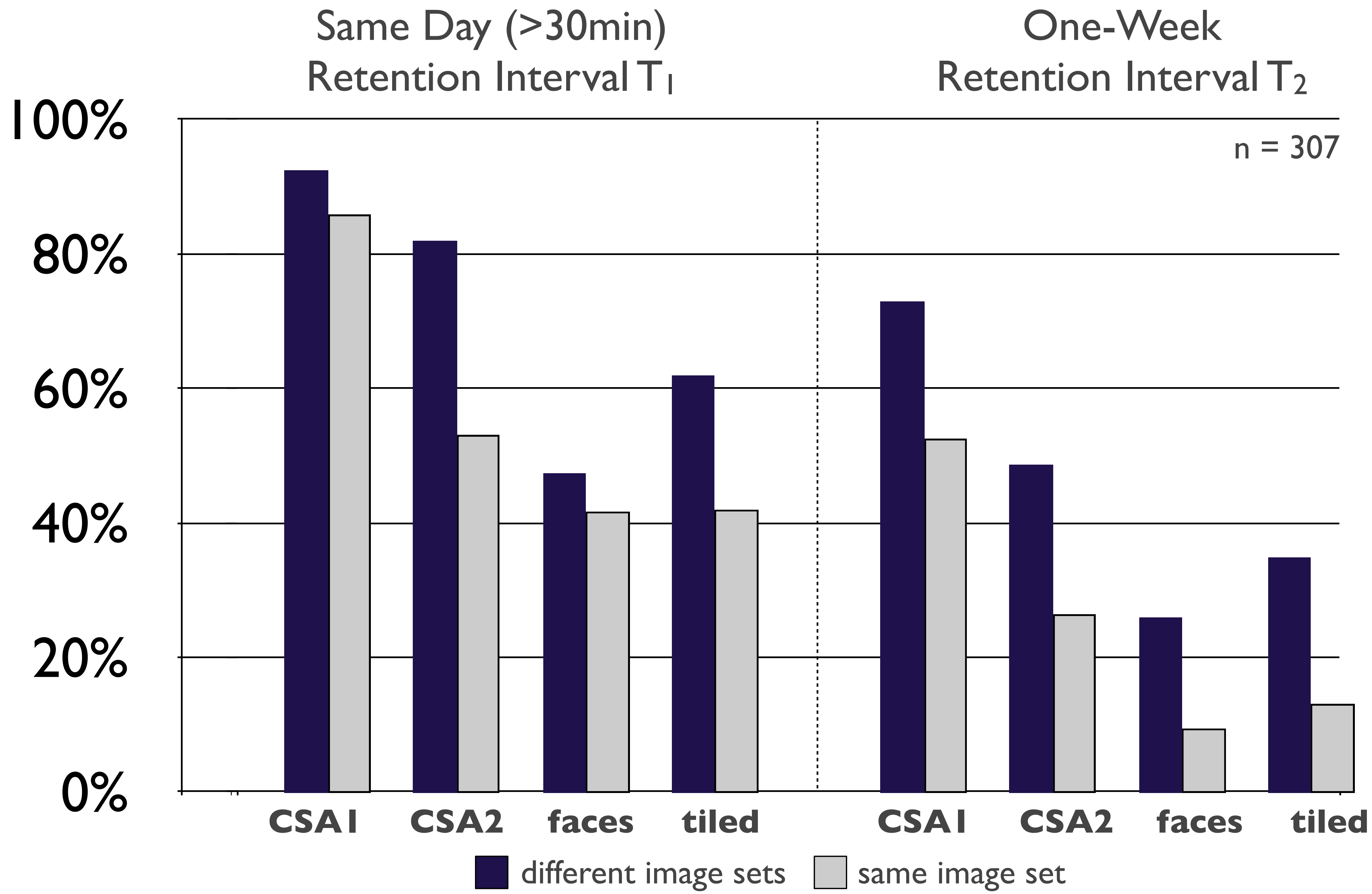


Long-Term Retention of Passwords



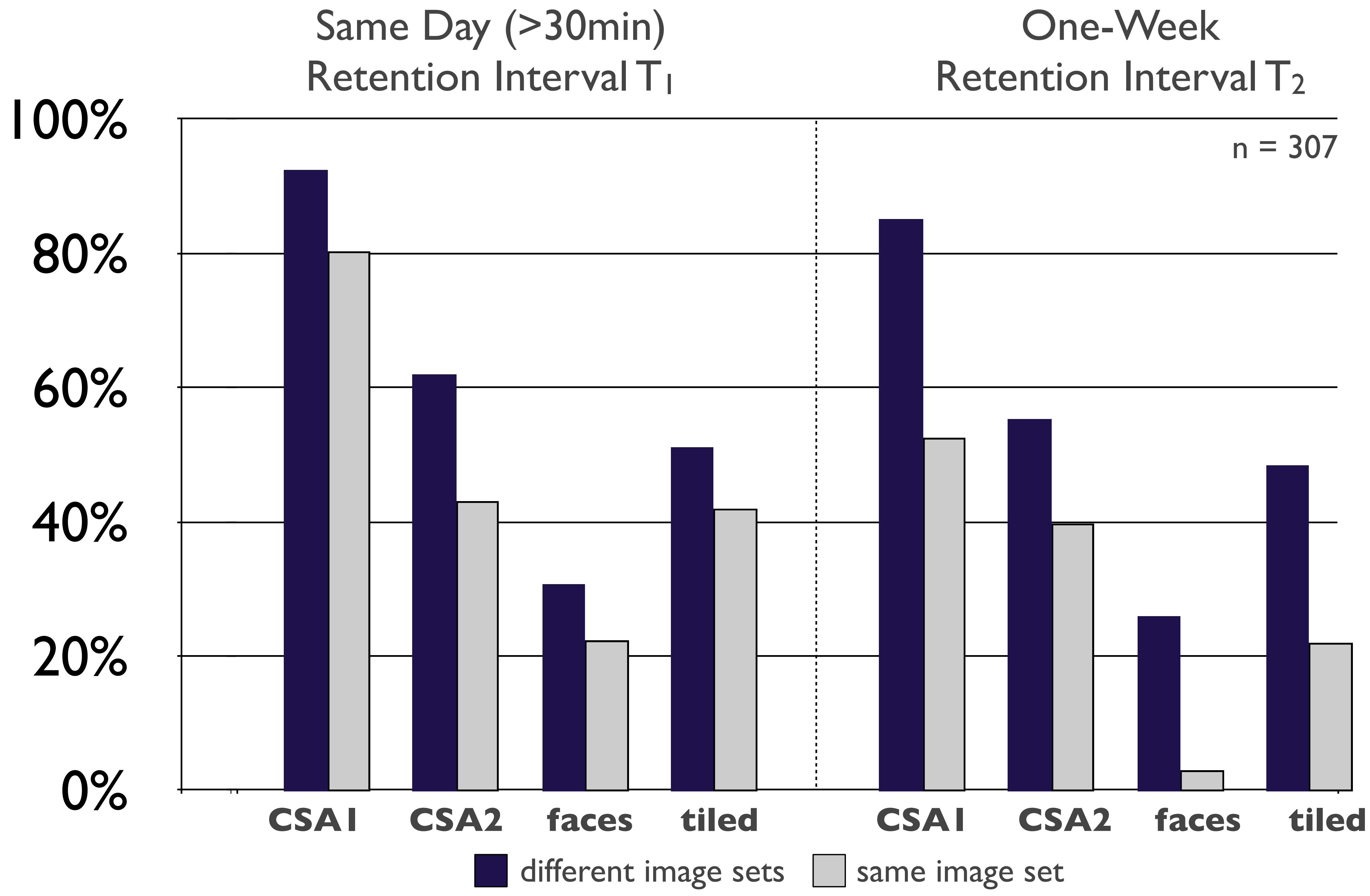
University of Idaho
A LEGACY OF LEADING

Authentication Success for *First* Graphical Password

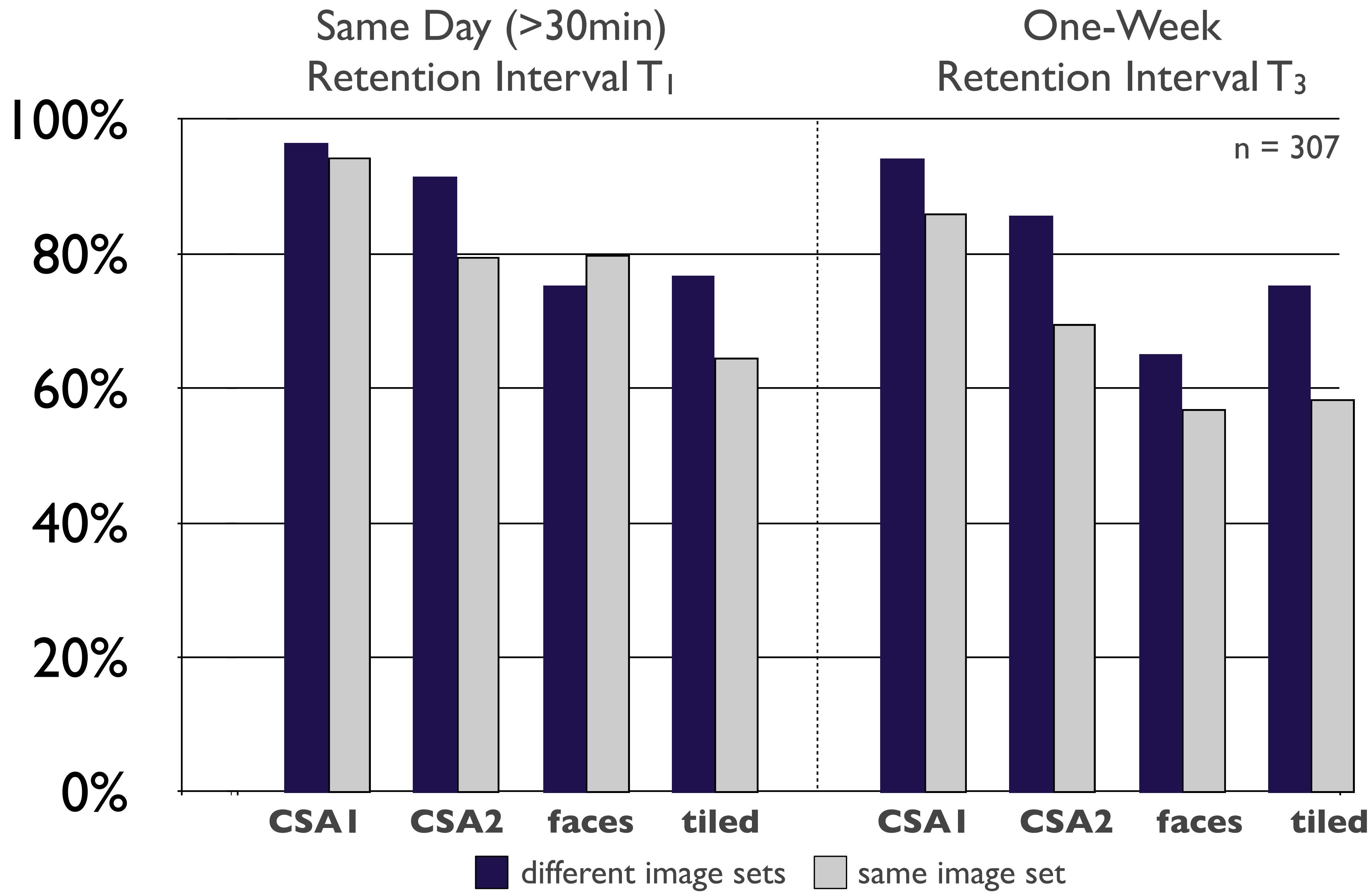


University of Idaho
A LEGACY OF LEADING

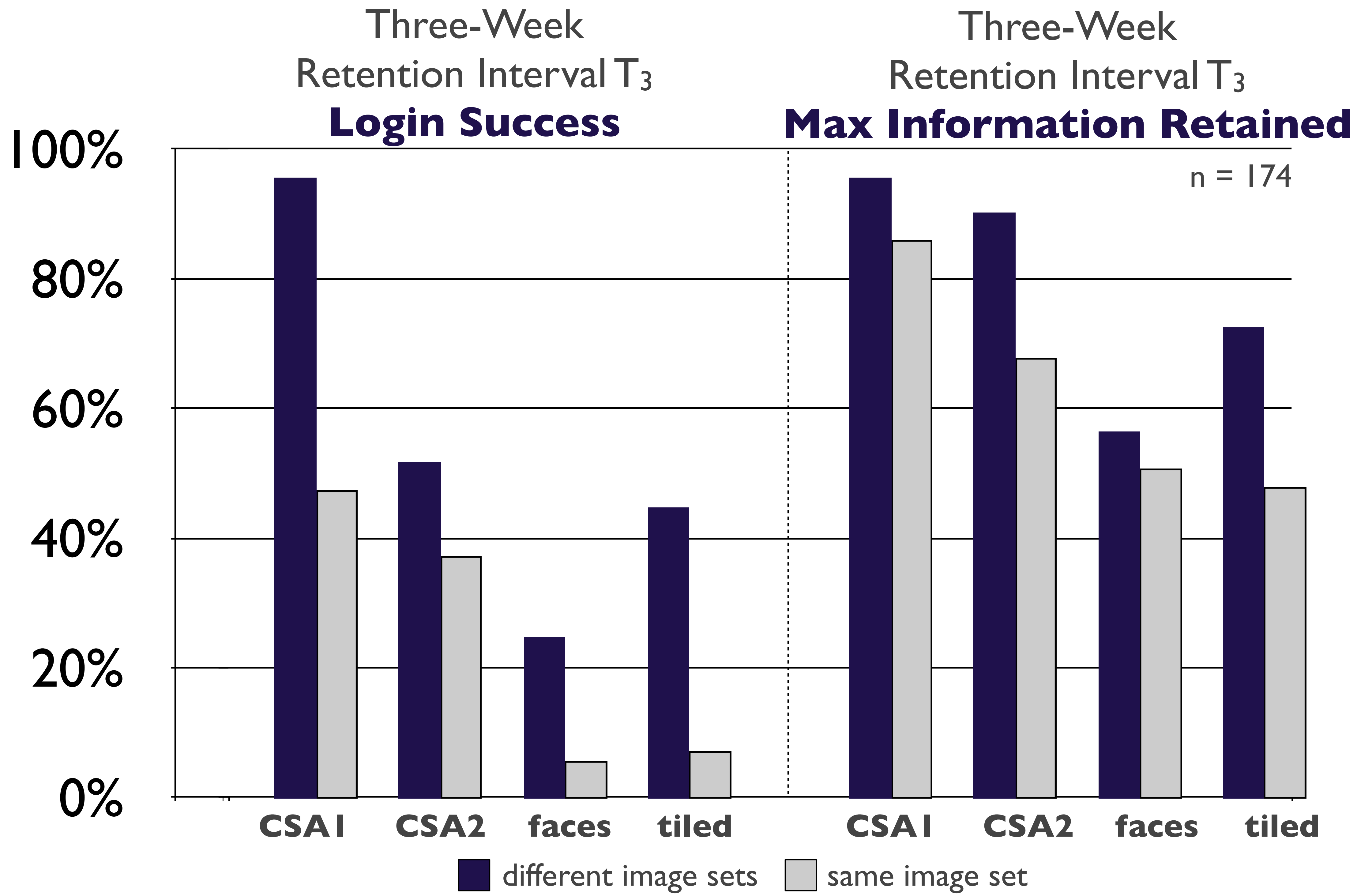
Authentication Success for *Second* Graphical Password



Max Information Retained (Both Graphical Passwords)



Long-Term Retention of Passwords



University of Idaho
A LEGACY OF LEADING

Scene context helps!
Different image sets help!

(Passwords based solely on faces don’t scale up)
Alphanumeric passwords expectedly perform worst

Visual Search in Visually or Categorically homogeneous/heterogeneous Item Sets

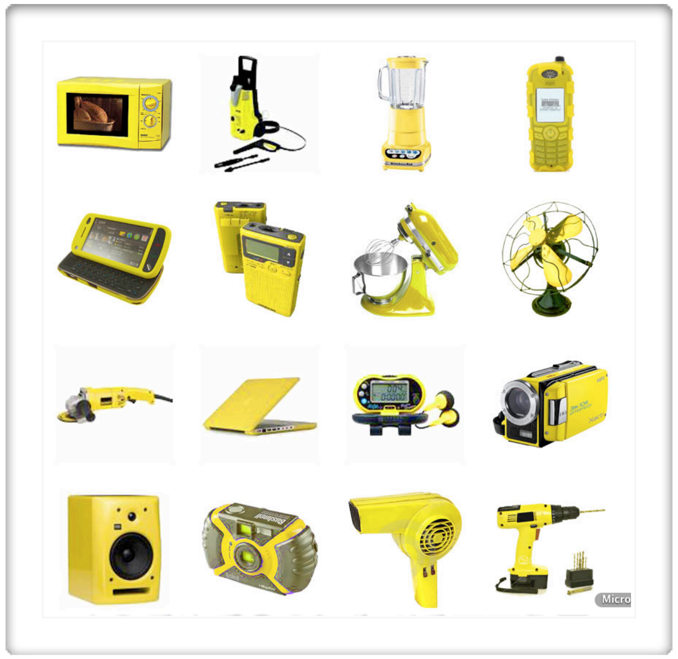
- **Variation of memory set size**
  - Participants had to remember **1, 3, or 9 dissimilar items** (presented for 5, 15, or 45 sec per set)
  - Each item in memory set belonged to a different category
  - Each item in memory set had a different color
- **2x2 Variation of visual search set**
  - **homogeneous color vs. heterogeneous color**
  - **homogenous vs. heterogeneous category set**
- **Blocked Search Trials**
  - for each memory set, 32 blocked search trials (50% present)

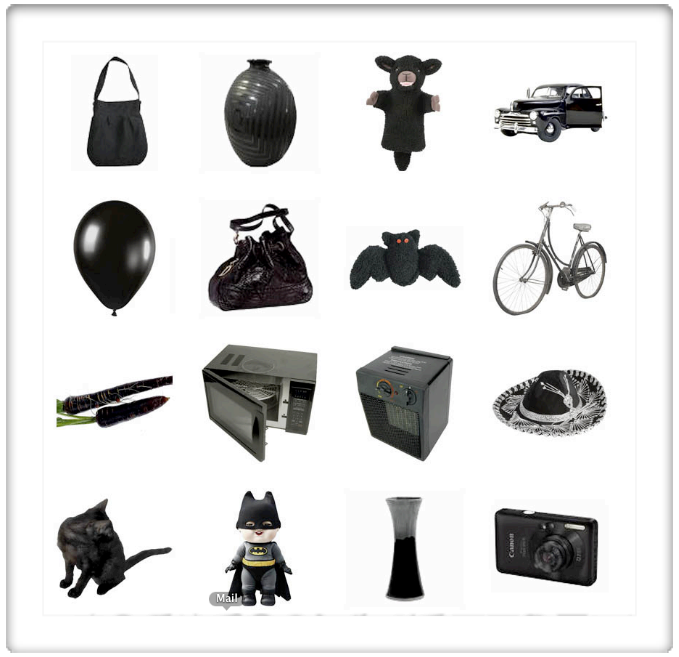
Visual Search in Visually or Categorically homogeneous/heterogeneous Item Sets

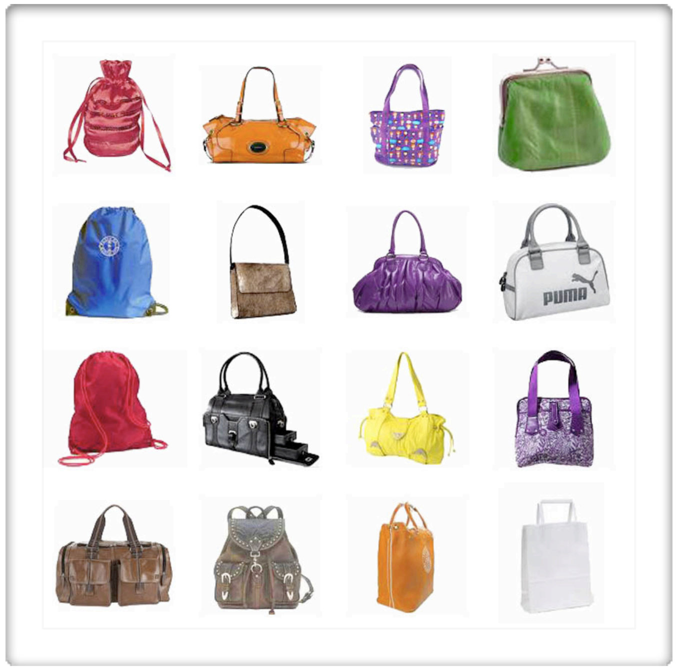
- **Participants**
  - 29 UI undergraduate student volunteers
  - 16 females, 13 males
  - Ages 18-52 (M = 22.3, SD = 6.1)
  - Normal visual acuity and color vision
- **Material**
  - 9 categories * 9 colors * 17 exemplars = 1,377 images
  - From database (Art Explosion Photo Objects 150,000), image searches
  - Base colors homogenized (Adobe Photoshop)

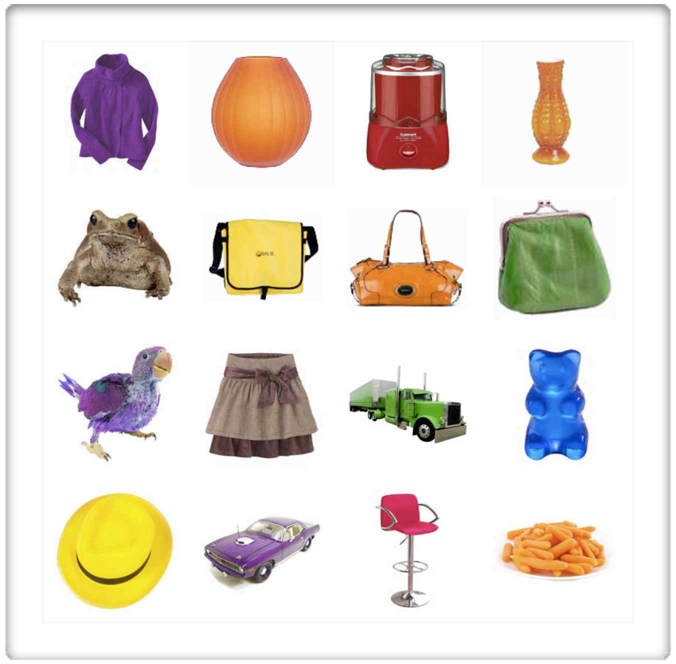
Memory Sets

Search Screens

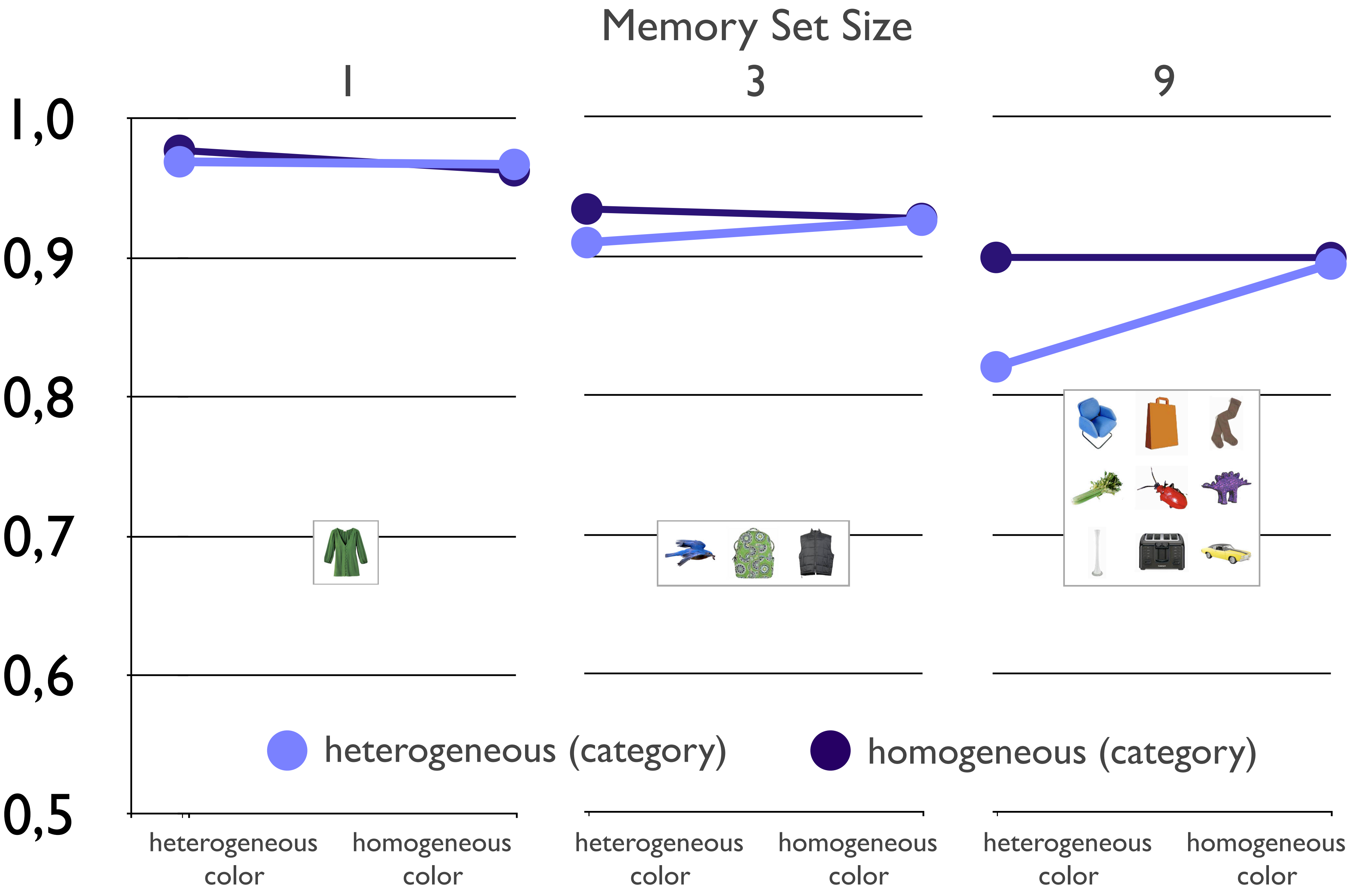




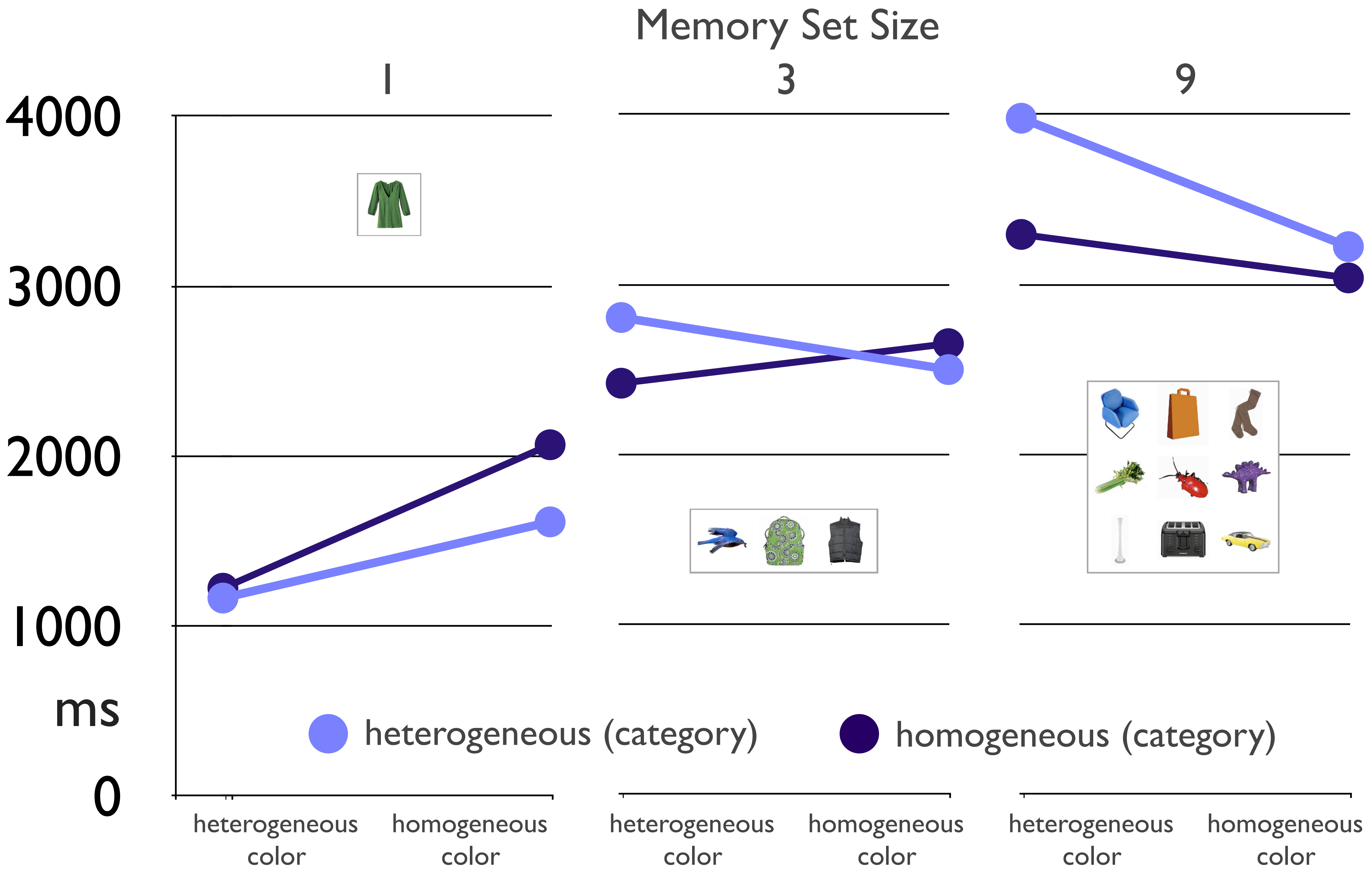




Correct Responses by Condition



Response Times by Condition



Categories Matter!

(and so do visual features)

Authentication by Category and Composite Scene Authentication (CSA)

constant password strength = 36 bit

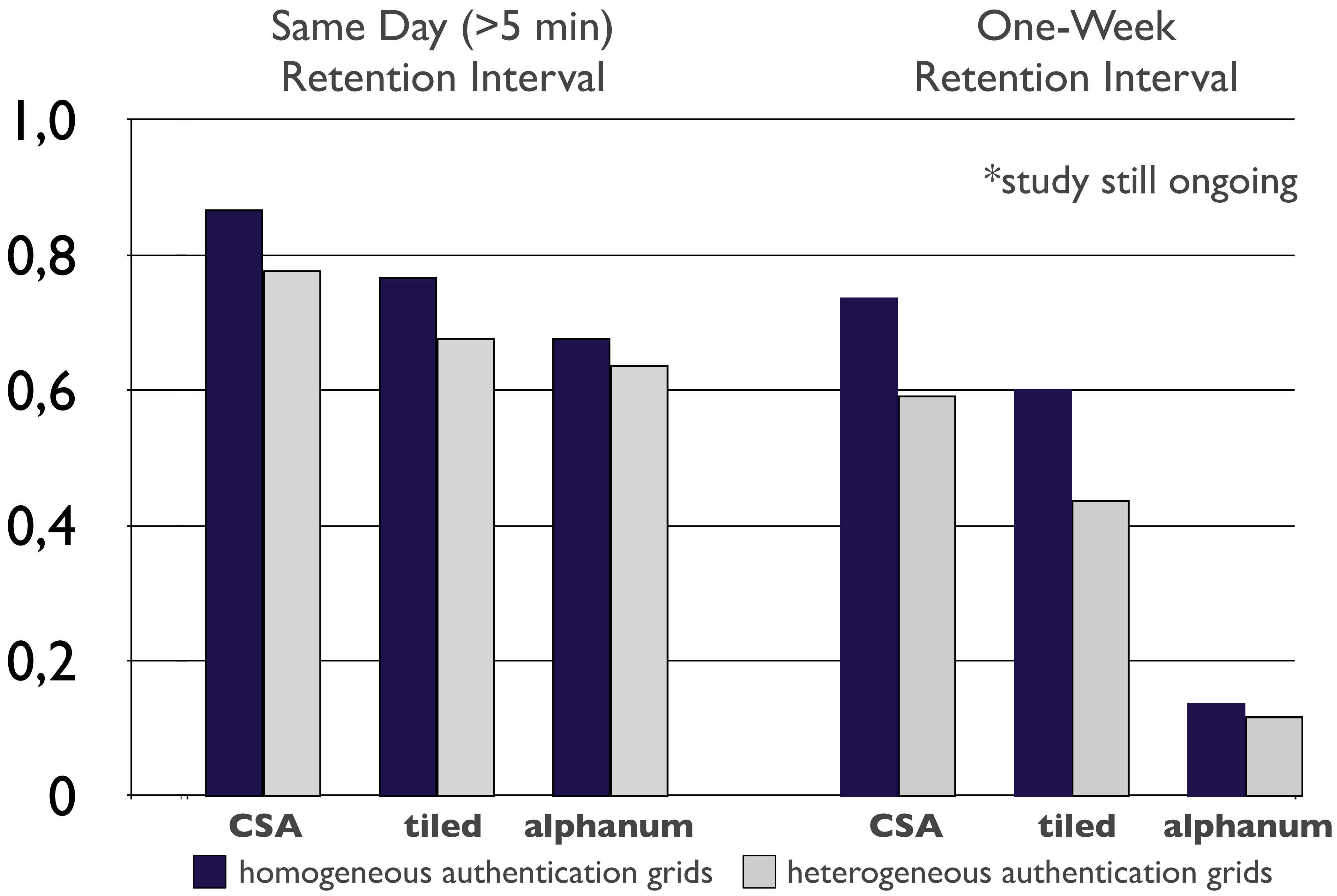
- **1 variation of CSA**
  - **CSA serial + composite**
- **1 alternative graphical authentication systems**
  - **Tiled** (VIP, De Angeli et al. 2005)
- **2 graphical passwords (same type) to remember**
  - disambiguated through visual/semantic context and challenge screens (always different sets of images)
- **2 alphanumeric passwords to remember**
  - disambiguated through visual/semantic context
- **Categorical / no-categorical organization of authentication screens**

Authentication by Category and Composite Scene Authentication (CSA)

constant password strength = 36 bit

- **Participants**
  - 110 UI undergraduate student volunteers participated in T_1 and T_2
  - 19 participants were excluded because of independent memory criterion
  - Ages 18-29 (M = 20.6, SD = 2.2)
  - All but 1 reported normal (or corrected to normal) vision
  - All reported normal memory
- **Material**
  - Images from database used by Johnson and Werner (2006) split into 2 distinct pools
  - Passcodes (CSA, tiled, alphanumeric)
  - PHP website for testing and data collection
  - Short story and list of words for filler task

Authentication Success by Condition*



*study still ongoing

Categories matter in authentication, too!

(scene context helps, too)

Strengths of Composite Scene Authentication (CSA)

- **For 1 week retention interval,**
  - Categorically organized authentication screens create approximately **+10% successful login rate improvement**
  - Scene context creates approximately another **+10% successful login rate improvement** over alternative systems
  - longer retention intervals might lead to even higher benefits
- **Restriction to semantically deficient images (faces, abstract images) leads to comparably poor performance**
- **Spatial passwords fare poorly (in our studies)**
  - Role of procedural memory might show benefit when used often & regularly
- **Well designed graphical authentication shows greatly improved performance over alphanumeric passwords**

Open Questions

- **Usability**
  - Speed of entry
  - Prevention of shoulder-surfing
  - Use on mobile devices
- **Cost-benefit analysis of memory set vs. search screen size**
- **Scalability - under which circumstances do graphical passwords interfere with each other?**

Thanks

Korey Johnson
Sergio Caltagirone
Kylie Pfeifer
Michael Teske

usercentric
United States Government
hp
invent
University of Idaho

THE UNIVERSITY OF IDAHO

1889