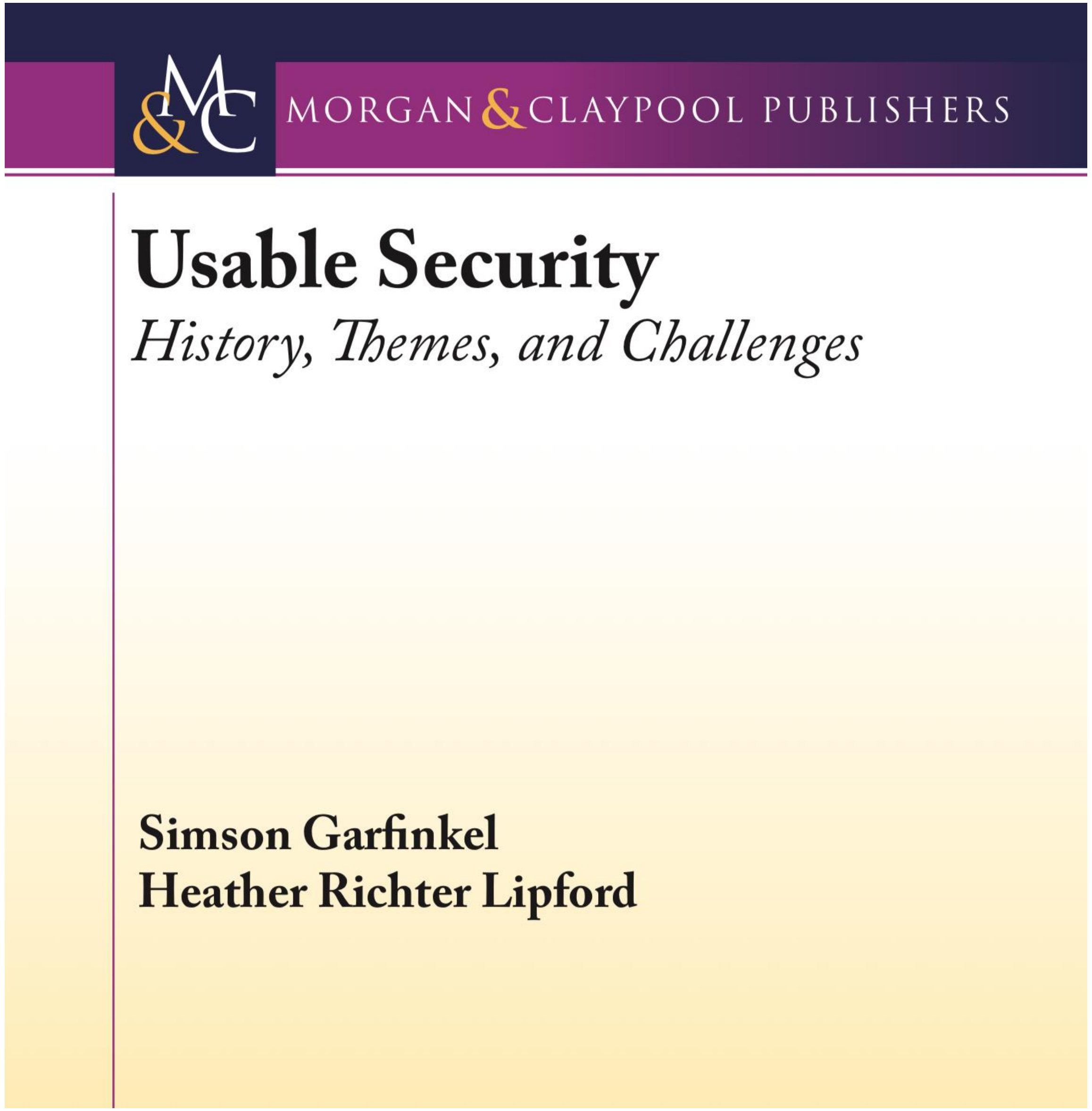
Usable Security

Sebastian Schrittwieser

Edgar Weippl

Reading

- Symposium on Usable Privacy and Security (SOUPS)
- Workshop on Usable Security (Usec)
- ACM CHI
- Usable Security (Garfinkel, Lipford)



MORGAN & CLAYPOOL PUBLISHERS

Usable Security

History, Themes, and Challenges

Simson Garfinkel
Heather Richter Lipford

Major Topics

- User Authentication
- E-Mail Security
- Anti-Phishing
- Storage
- Device Pairing
- Web Privacy
- Policy Specification and Interaction
- Mobile Security and Privacy
- Social Media Privacy
- Security Administrators

Basics

- “usable security” is a more colloquial meaning of aligning research in HCI with computer security.
- Usability and security once were inherently antagonistic.
- Today: systems that are not usable will inevitably suffer security failures when deployed in the real world.

- Can you think of examples?

Usable Security has been important … for quite a while

- In 2003, the Computing Research Association identified the **need for usable security**
- Hence, achieving **better training** and identifying how to create usable security software for both end-users and system administrator.
- **Unfair blame** on users for the security mishaps.
- Attention to usability in building secure systems goes back near 4 decades identifying "**psychological acceptability**" as a principle in computing environment

5 Properties

1. The **unmotivated user** who would rather send email, browse web pages or work.
2. **Abstraction Property**: Security properties seem too abstract for users
3. Lack of **Feedback Property**: Users do not ”see“ bad security behavior
4. **Barn Door Property**: Data theft cannot be easily detected ”because it‘s still there“
5. **Weakest Link Property**: A single error may suffice

Why is it hard?

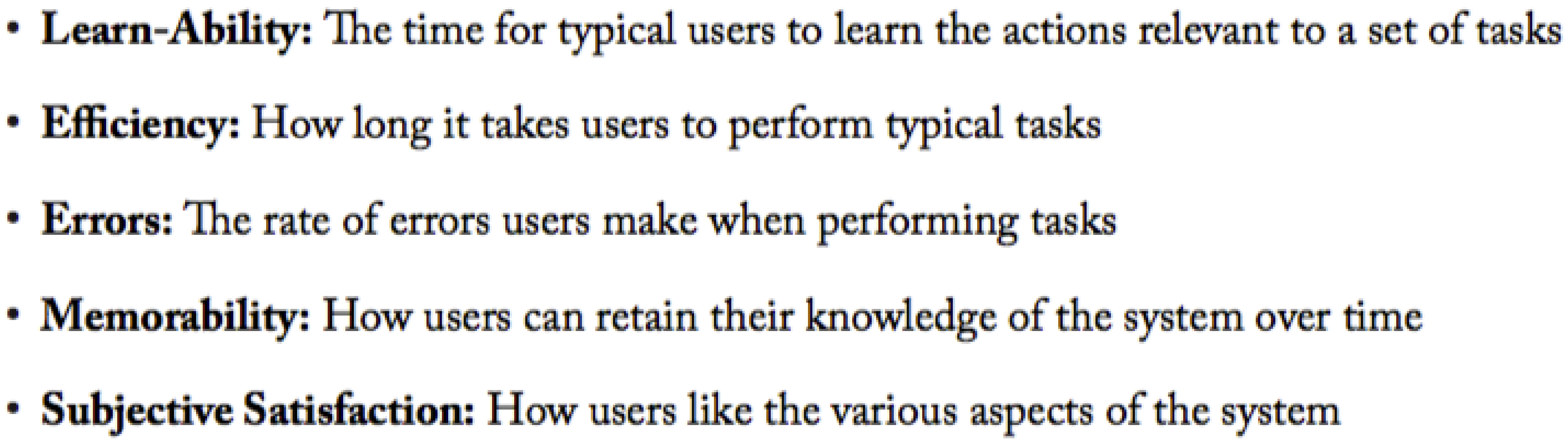
- **Interdisciplinary Challenge**: HCI vs. Security
- **Challenge of Familiarity**: Good solutions are not appreciated enough
- **Interrelation Challenge**: Understanding the trade-offs is hard
- The **User Evaluation Challenge**: Users may think that e.g. typing a password often is more secure vs. Using OpenID

Why is it hard?

- The **Ecological Validity Challenge**: Lab studies vs. real-world. Studies have to trick users
- **Adversary Modeling Challenge**: difficult to assess user‘s perception of attackers. They might not cooperate since they think attackers will only attack “bigger fish“
- **Technology Velocity Challenge**: Systems change to fast and once studies are done may be obsolete and then hard to publish
- **Customer Challenge**: Vendors do not compete on who has the best TLS implementation.

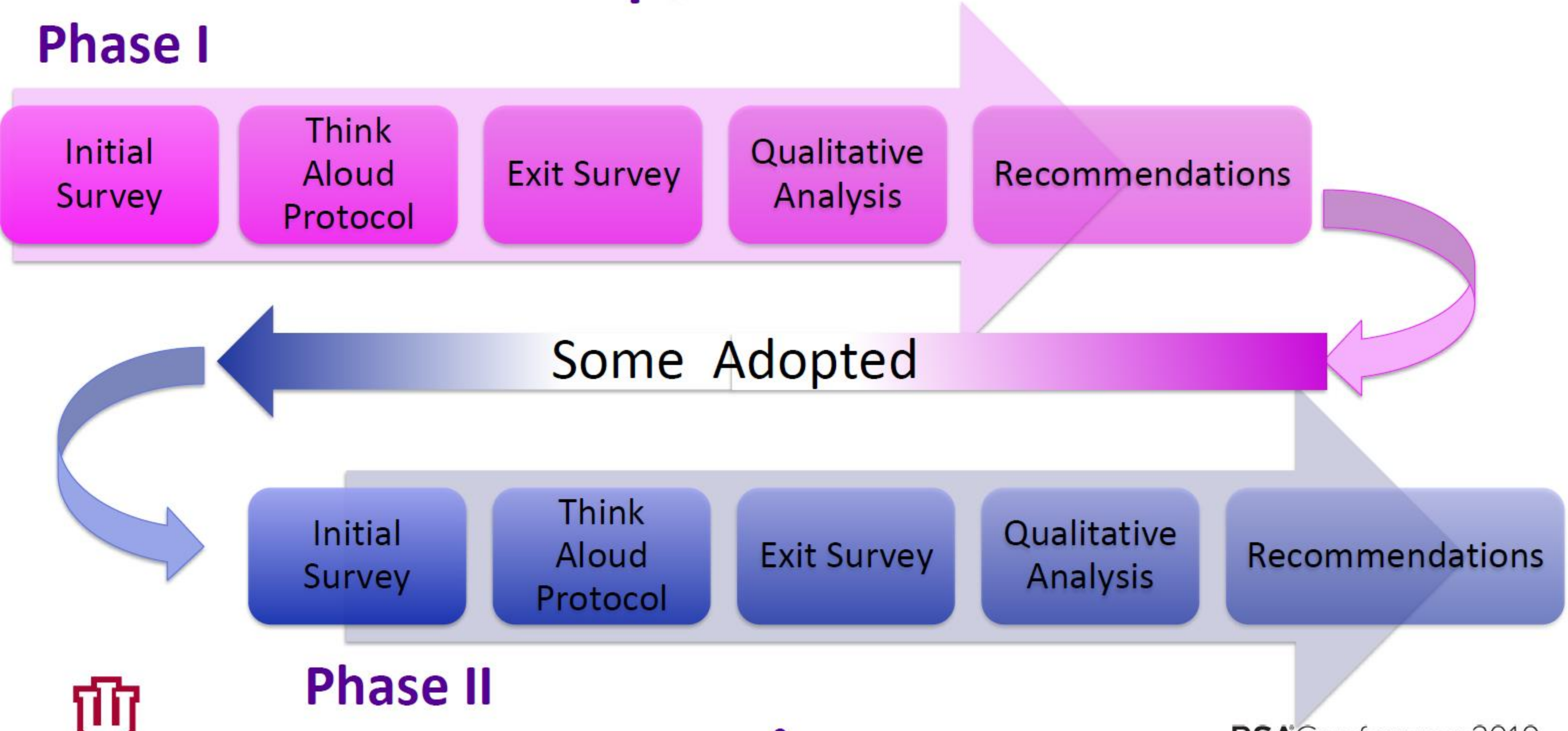
Usability

Usability is defined as “the extent to which a product can be used by specified user to achieve specified goal with effectiveness, efficiency, and satisfaction in a specified context of use”.



- **Learn-Ability:** The time for typical users to learn the actions relevant to a set of tasks
- **Efficiency:** How long it takes users to perform typical tasks
- **Errors:** The rate of errors users make when performing tasks
- **Memorability:** How users can retain their knowledge of the system over time
- **Subjective Satisfaction:** How users like the various aspects of the system

Identical Experimental Protocol



Phase I

Initial Survey

Think Aloud Protocol

Exit Survey

Qualitative Analysis

Recommendations

Some Adopted

Initial Survey

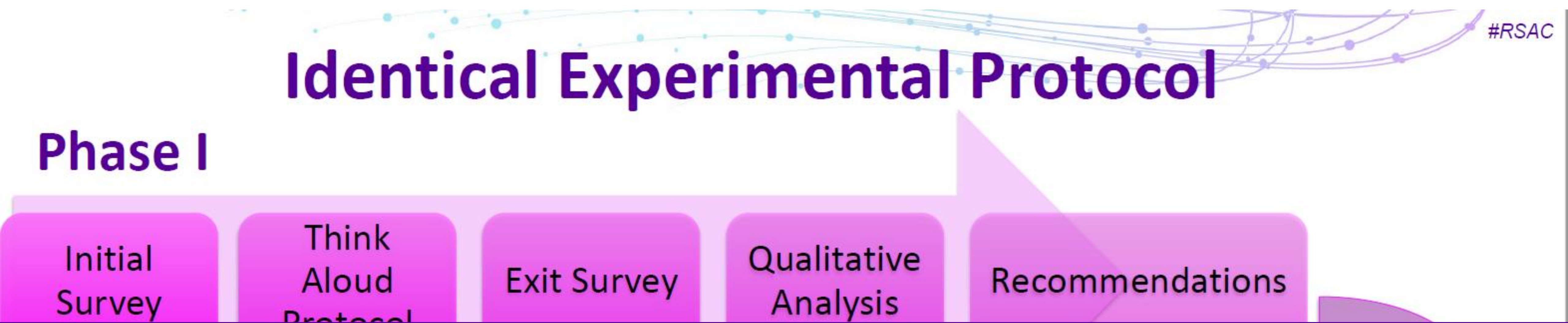
Think Aloud Protocol

Exit Survey

Qualitative Analysis

Recommendations

Phase II



#RSAC

Identical Experimental Protocol

Phase I

Initial Survey

Think Aloud Protocol

Exit Survey

Qualitative Analysis

Recommendations

SESSION ID: SEM-M01

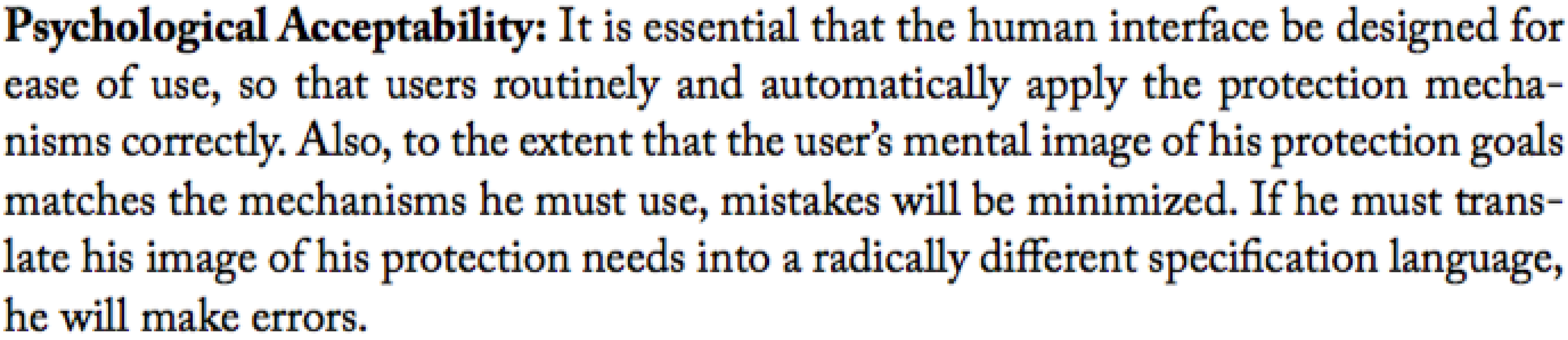
Humanistic Multi-Factor Authentication (MFA)
Why We Don't Use MFA

Sanchari Das

Doctoral Candidate
Indiana University Bloomington
@sancharidecrypt

Early Work (1975-1995)

psychological acceptability (Salzer and Schroeder 1975)



Psychological Acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors.

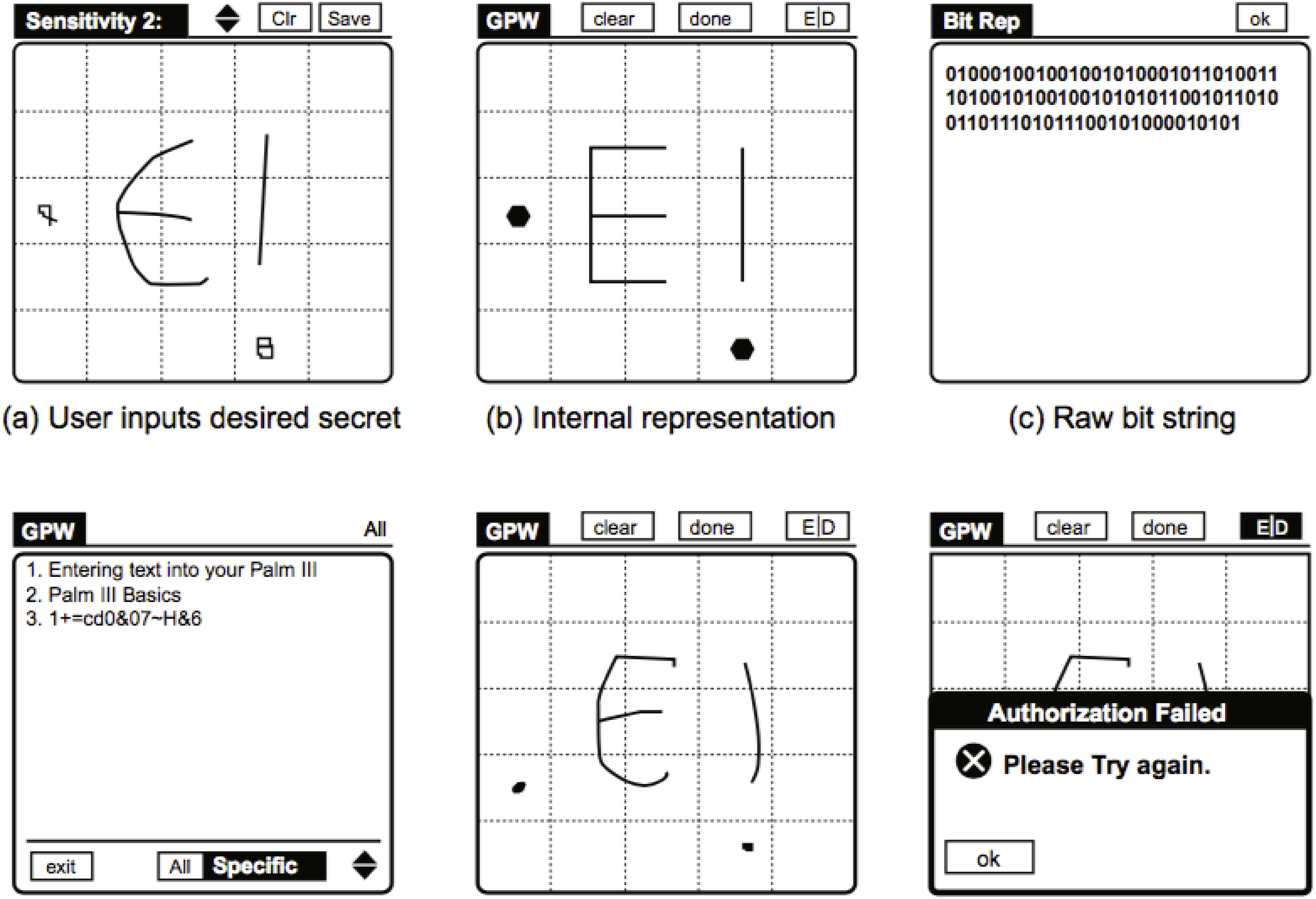
Early Work (1975-1995)

- Psychological acceptability has the user interface aspect that promotes ease-of-use, and correspondence between internal system mechanisms and user mental models.
- Computers make 2 errors
  - Slips - user’s intention is correct but not the execution.
  - Mistakes - user’s intended action was itself an error.

The Birth of UPS (1995-2000)

Landmark papers

- Why Johnny Can‘t Encrypt
  - https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50
- Users are not the enemy
  - https://dl.acm.org/citation.cfm?id=322806
- The Design and Analysis of Graphical Passwords
  - https://www.usenix.org/legacy/events/sec99/full_papers/jermyn/jermyn.pdf



```
010001001001001010001011010011
101001010010010101011001011010
011011101011100101000010101
```

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&07~H&6

Authorization Failed

Please Try again.

(a) User inputs desired secret

(b) Internal representation

(c) Raw bit string

(d) Interface to database

(e) Re-entry of (incorrect) secret

(f) Authorization failed

What do the papers say?

- We need to understand and improve technical failings of today‘s tools
- User modeling
- Development and evaluation of authentication as starting point

Password Research

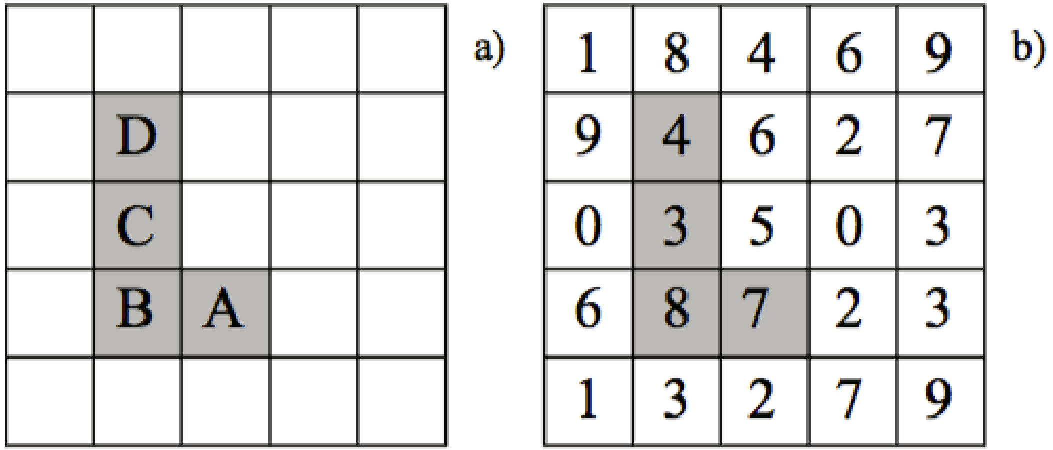
- Studies of password policies
- Retrospective studies of password databases that were stolen and publicly leaked
- Lab and field studies of users who are tasked with picking and using a a password
- Field studies of actual password usage on operational systems

Graphical Passwords

- Draw-A-Secret
- Remember a set of images
- Set of points on an image

Current Methods

- Biometrics
- Time-based One-Time Passwords
- Challenge-Response Authentication
- Mental Computation



	D			
	C			
	B	A		

1	8	4	6	9
9	4	6	2	7
0	3	5	0	3
6	8	7	2	3
1	3	2	7	9

Figure 3.9: The GrIDsure system. a) Users enroll by picking four cells (in this case, A, B, C and D). b) users authenticate by typing the numbers shown in the chosen cells (in this case, 7834). (Based on Brostoff et al. [2010].)

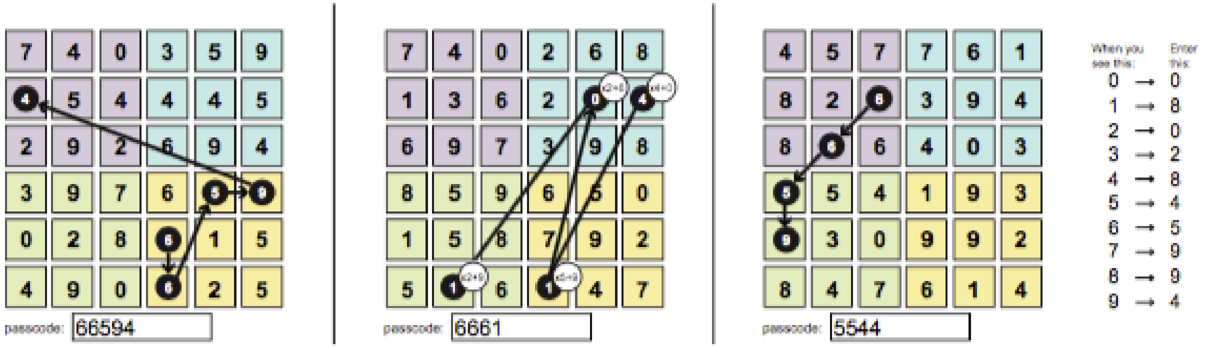
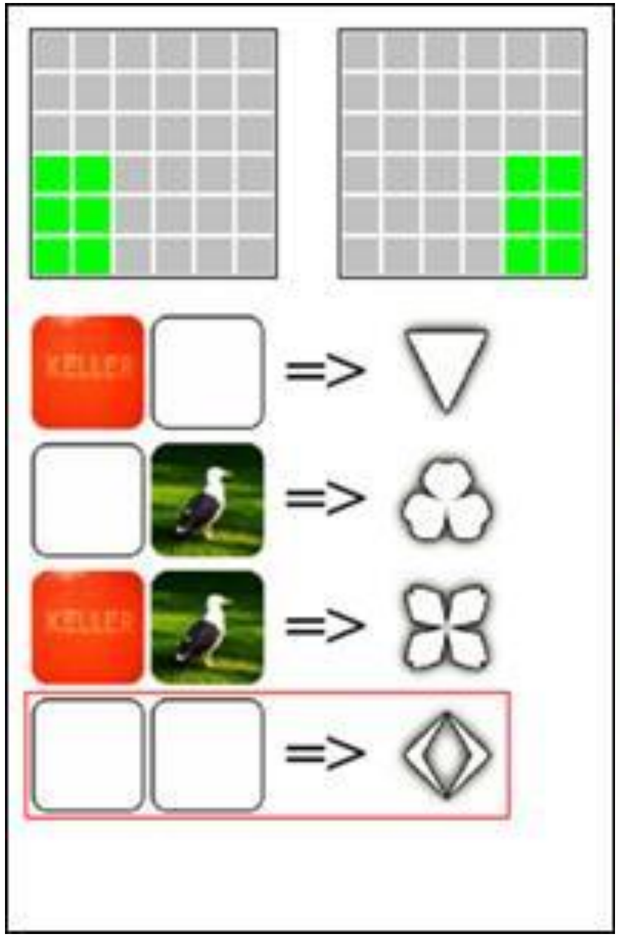
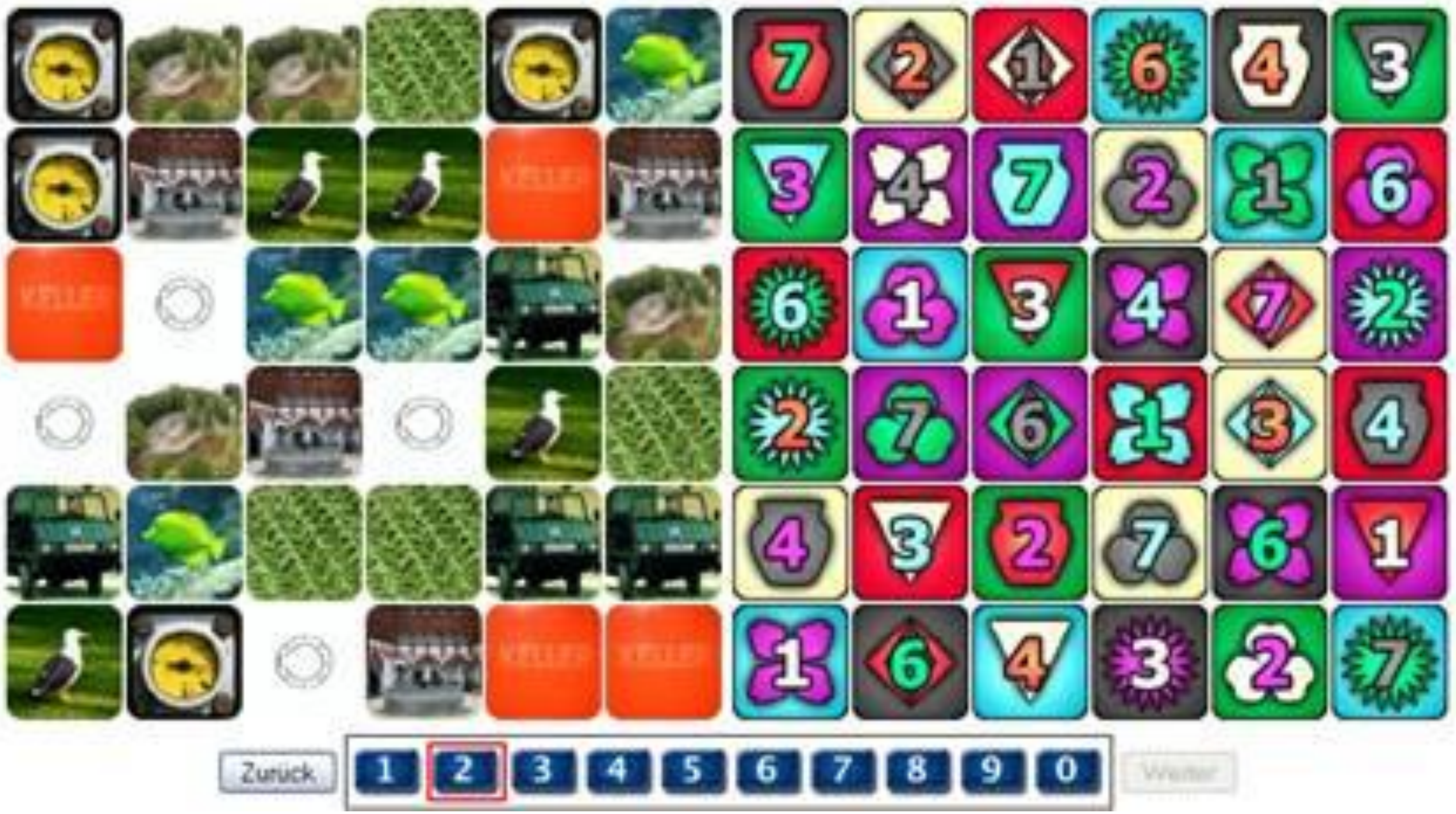


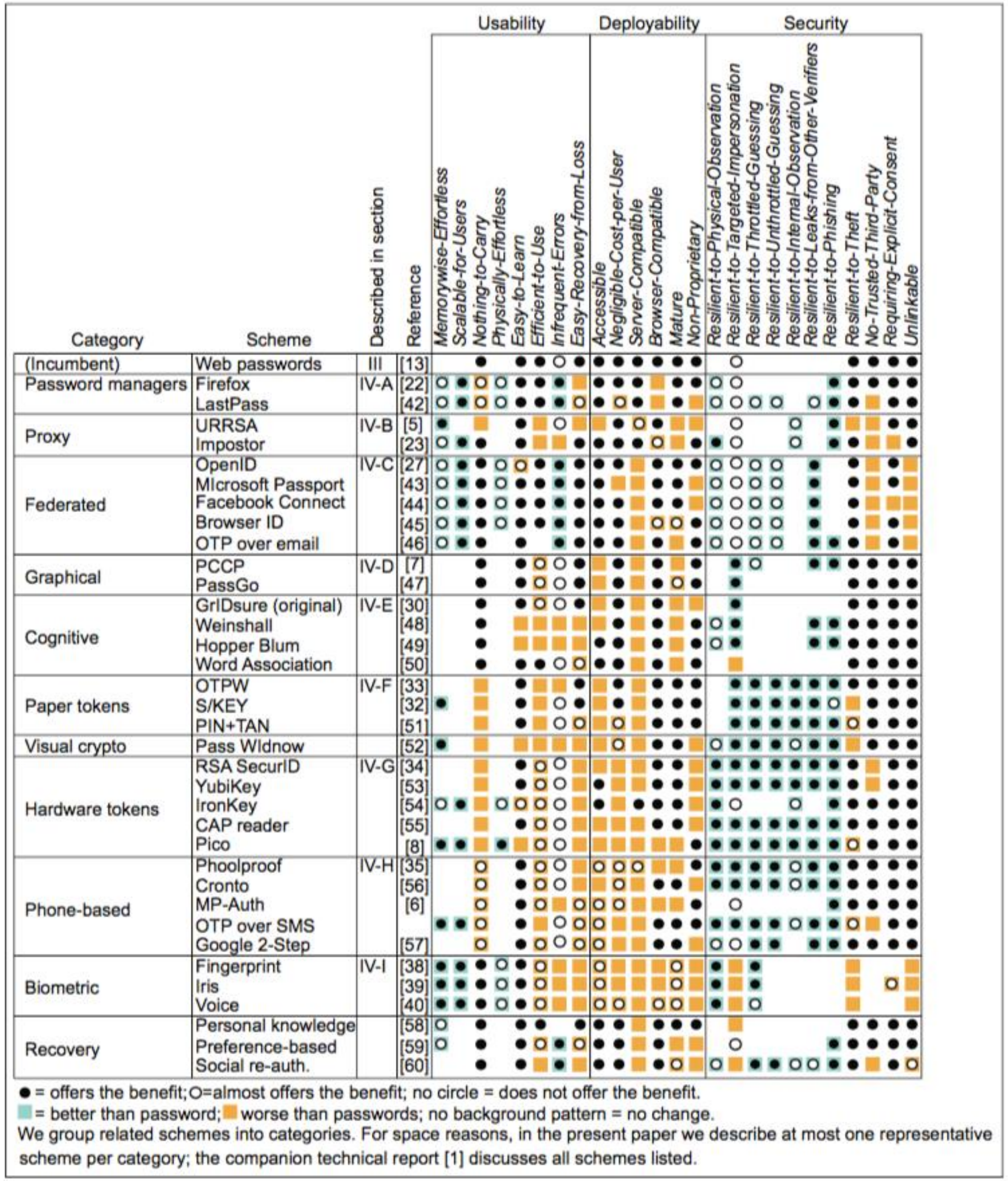
Figure 3.10: Kelley et al. [2013b] increase the security of the GrIDsure system by adding mental arithmetic that the user must perform before entering their passcode.

SecLookOn


KELLER
=>
=>
KELLER
=>
=>


KELLER
KELLER
KELLER
KELLER
7 2 1 6 4 3
3 4 7 2 1 6
6 1 3 4 7 2
2 7 6 1 3 4
4 3 2 7 6 1
1 6 4 3 2 7
Zurück
1
2
3
4
5
6
7
8
9
0
Weiter

Survey Papers



				Usability								Deployability						Security										
Category	Scheme	Described in section	Reference	*Memorywise-Effortless*	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	🟩○	🟩●	🟧○	🟩○	●	●	🟩●	🟧	●	●	●	🟧	●	●	🟩○	○					🟩●	●	●	●	●
	LastPass		[42]	🟩○	🟩●	🟧○	🟩○	●	●	🟩●	🟧○	●	🟧○	●	🟧	●	🟧	🟩○	○	🟩○	🟩○		🟩○	🟩●	●	🟧	●	●
Proxy	URRSA	IV-B	[5]	🟩●		🟧		●	🟧	○	🟧	🟧	●	🟧○	●	🟧	🟧		○			🟩○		🟩●	🟧	🟧	●	●
	Impostor		[23]	🟩○	🟩●	●		●	🟧	🟧	●	●	●	●	🟧○	🟧	●	🟩●	○			🟩○		🟩●	●	🟧	🟧	●
Federated	OpenID	IV-C	[27]	🟩○	🟩●	●	🟩○	🟧○	●	🟩●	●	●	●	🟧	●	●	●	🟩○	○	🟩○	🟩○		🟩●		●	🟧	●	🟧
	MIcrosoft Passport		[43]	🟩○	🟩●	●	🟩○	●	●	🟩●	●	●	🟧	🟧	●	●	🟧	🟩○	○	🟩○	🟩○		🟩●		●	🟧	●	🟧
	Facebook Connect		[44]	🟩○	🟩●	●	🟩○	●	●	🟩●	●	●	●	🟧	●	●	🟧	🟩○	○	🟩○	🟩○		🟩●		●	🟧	🟧	🟧
	Browser ID		[45]	🟩○	🟩●	●	🟩○	●	●	🟩●	●	●	●	🟧	🟧○	🟧○	●	🟩○	○	🟩○	🟩○		🟩●		●	🟧	●	🟧
	OTP over email		[46]	🟩○	🟩●	●		●		🟩●	●	●	●	🟧	●	🟧	●	🟩○	○	🟩○	🟩○		🟩●	🟩●	●	🟧	●	🟧
Graphical	PCCP	IV-D	[7]			●		●	🟧○	○	●	🟧	●	🟧	●	🟧	●		🟩●	🟩○			🟩●	🟩●	●	●	●	●
	PassGo		[47]			●		●	🟧○	○	●	🟧	●	🟧	●	🟧○	●		🟩●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	🟧○	○	●	🟧	●	🟧	●	🟧	🟧		🟩●						●	●	●	●
	Weinshall		[48]			●		🟧	🟧	🟧	🟧	🟧	●	🟧	●	🟧	●	🟩○	🟩●				🟩●	🟩●	●	●	●	●
	Hopper Blum		[49]			●		🟧	🟧	🟧	🟧	●	●	🟧	●	🟧	●	🟩○	🟩●				🟩●	🟩●	●	●	●	●
	Word Association		[50]			●		●	●	○	🟧○	●	●	🟧	●	🟧	●		🟧						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			🟧		●	🟧	🟧	●	🟧	●	🟧	●	●	●		🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	●	●	●	●
	S/KEY		[32]	🟩●		🟧		●	🟧	○	●	🟧	●	🟧	●	●	●		🟩●	🟩●	🟩●	🟩●	🟩●	🟩○	🟧	●	●	●
	PIN+TAN		[51]			🟧		●	🟧	○	🟧○	🟧	🟧○	🟧	●	●	●		🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟧○	●	●	●
Visual crypto	Pass WIdnow		[52]	🟩●		🟧		🟧	🟧	🟧	🟧	🟧	🟧○	🟧	●	●	🟧	🟩○	🟩●	🟩●	🟩●	🟩○	🟩●	🟩●	🟧	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			🟧		●	🟧○	○	🟧	🟧	🟧	🟧	●	●	🟧	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	●	🟧	●	●
	YubiKey		[53]			🟧		●	🟧○	○	🟧	●	🟧	🟧	●	●	🟧	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	●	🟧	●	●
	IronKey		[54]	🟩○	🟩●	🟧	🟩○	🟧○	🟧○	○	🟧	●	🟧	●	●	●	🟧	🟩●	○			🟩○		🟩●	●	●	●	●
	CAP reader		[55]			🟧		●	🟧○	○	🟧	🟧	🟧	🟧	●	●	🟧	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	●	●	●	●
	Pico		[8]	🟩●	🟩●	🟧	🟩●	🟧	🟧○	○	🟧	🟧	🟧	🟧	🟧	🟧	●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟧○	●	●	●
Phone-based	Phoolproof	IV-H	[35]			🟧○		●	🟧○	○	🟧	🟧○	🟧○	🟧○	🟧	🟧	●	🟩●	🟩●	🟩●	🟩●	🟩○	🟩●	🟩●	●	●	●	●
	Cronto		[56]			🟧○		●	🟧○	○	🟧	🟧	🟧○	🟧	●	●	🟧	🟩●	🟩●	🟩●	🟩●	🟩○	🟩●	🟩●	●	●	●	●
	MP-Auth		[6]			🟧○		●	🟧○	🟧	🟧○	🟧○	🟧○	🟧	🟧	🟧	●		○					🟩●	●	●	●	●
	OTP over SMS			🟩●	🟩●	🟧○		●	🟧	○	🟧○	🟧○	🟧	🟧	●	●	●	🟩●	🟩●	🟩●	🟩●	🟩○	🟩●	🟩●	🟧○	🟧	●	●
	Google 2-Step		[57]			🟧○		●	🟧○	○	🟧○	🟧○	🟧	🟧	●	●	🟧	🟩○	○	🟩●	🟩●		🟩●	🟩●	●	●	●	●
Biometric	Fingerprint	IV-I	[38]	🟩●	🟩●	●	🟩○	●	🟧○	🟧	🟧	🟧○	🟧	🟧	🟧	🟧○	🟧	🟩●	🟧	🟩●					🟧			🟧
	Iris		[39]	🟩●	🟩●	●	🟩○	●	🟧○	🟧	🟧	🟧○	🟧	🟧	🟧	🟧○	🟧	🟩●	🟧	🟩●					🟧		🟧○	🟧
	Voice		[40]	🟩●	🟩●	●	🟩○	●	🟧○	🟧	🟧	🟧○	🟧○	🟧	🟧○	🟧○	🟧	🟩●	🟧	🟩○					🟧			🟧
Recovery	Personal knowledge		[58]	🟩○		●		●	●		●	●	●	🟧	●	●	●		🟧						●	●	●	●
	Preference-based		[59]	🟩○		●		●	🟧○	🟩●	🟧○	●	●	🟧	●	🟧	🟧		○					🟩●	●	●	●	●
	Social re-auth.		[60]			●		●	🟧	🟩●	🟧	●	●	🟧	●	🟧○	🟧	🟩○	🟧	🟩●	🟩●	🟩○	🟩○	🟩●	●	🟧	●	🟧○

● = offers the benefit; ○=almost offers the benefit; no circle = does not offer the benefit.
🟩 = better than password; 🟧 worse than passwords; no background pattern = no change.
We group related schemes into categories. For space reasons, in the present paper we describe at most one representative scheme per category; the companion technical report [1] discusses all schemes listed.

Figure 3.5: Based on Bonneau et al. [2012b, Table 1].

RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: SEM-M01

The Quest for Usable and Secure Passwords

Lujo Bauer

Associate Professor of ECE & CS
Carnegie Mellon University
@lujobauer

Studies of password policies

- In 2010 Governments/universities had stricter policies than e-banking
- 2010: Prevent people from using frequently used passwords (count-min data structure – how would you securely implement that?)
- Mental models: finite amount of effort that user is capable of using for passwords. They group high value / low probabilty of compromise accounts and low value / high probability accounts.

Retrospective studies of password databases that were stolen and publicly leaked

- 4-digit ATM PIN
  - Blacklist about 100 PIN (0101, 0202, 1234, ...)
  - Reduce chance of breaking it with 6 guesses from 1.9% to 0.2%
  - Personal blacklist (birth dates, years, etc)

- Strong PW != Strong PW
  - People who create strong (=better than the policy requires) passwords create different kinds passwords than those forced to by technical controls.

- Ethical considerations

Lab and field studies of users who are tasked with picking and using a a password

- 16 char passwords chosen with no other restriction are as secure as 8 char passwords with 4-character classes enforced and dictionary check. → Longer passwords are not automatically better
- Password meters influence people to chose better passwords but the meters might not really measure passwords strength
- Real-world passphrases have a lot less entropy than expected.

Field studies of actual password usage on operational systems

Weaknesses of lab studies

- People might not care about lab studies as much as their e-banking
- People might use stronger passwords because they do not need to remember them long-term
- People be primed if they know they are being watched

- A study compared the real passwords (with the help of the IT departments) with passwords chosen in lab situation to measure how realistic lab environments are.
  - 1/3 pick unrealistic passwords
  - Lab is much better than online study
  - ¼ used their „real“ passwords in the lab

Fallback and Backup Authentication

- Challenge Question (what is your favorite color)
  - Applicability (does the question work for all people?)
  - Memorability
  - Repeatability (St. vs. Street)
- SMS, E-Mail, ...

Passwords are still a current topic…

ACM CCS 2017, Session B2: Passwords (3 papers)

…you do remember how to use the ACM digital library…

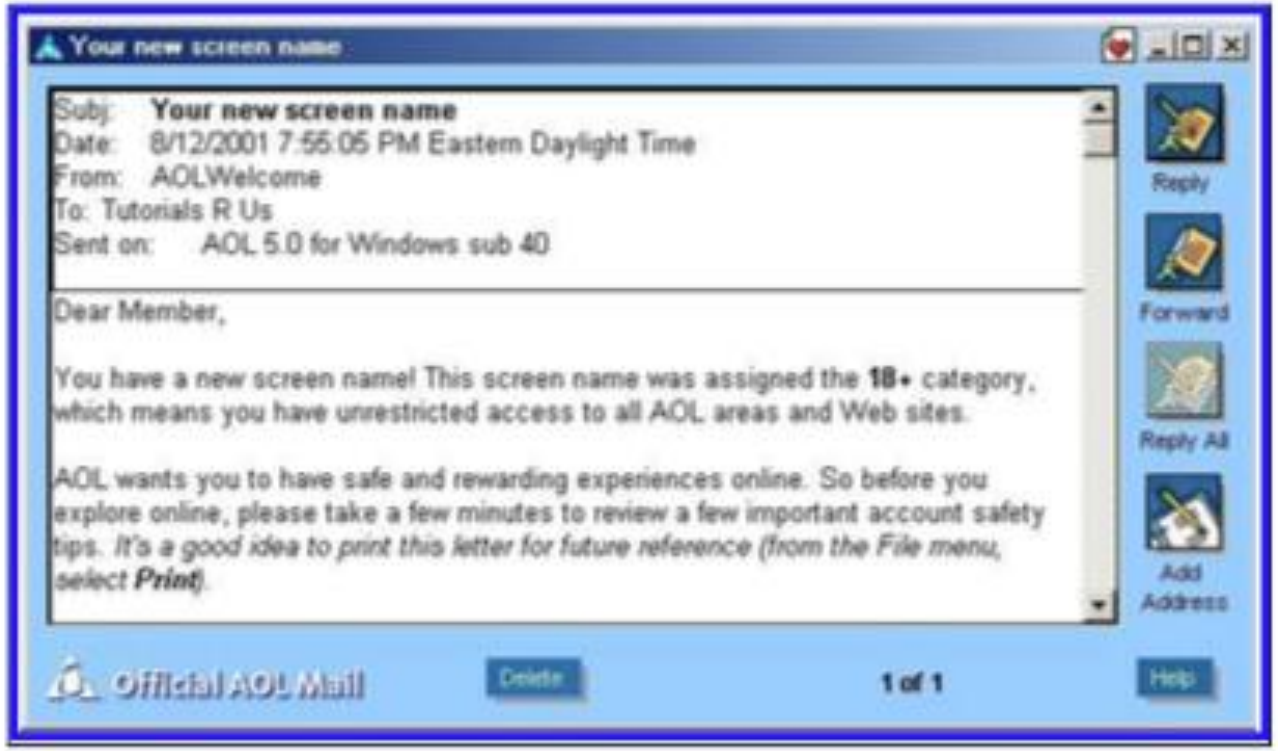
1. www.acm.org/dl
2. Proceedings
3. ACM CCS 2017
4. Table of Contents

Secure Messaging

- Signal
- Whatsapp

- Protocol vs. Implementation
- **Usability aspects**
  - What happens when a Person-in-the-middle is present?

Anti-Phishing 2003



Subj: **Your new screen name**
Date: 8/12/2001 7:55:05 PM Eastern Daylight Time
From: AOLWelcome
To: Tutorials R Us
Sent on: AOL 5.0 for Windows sub 40

Dear Member,

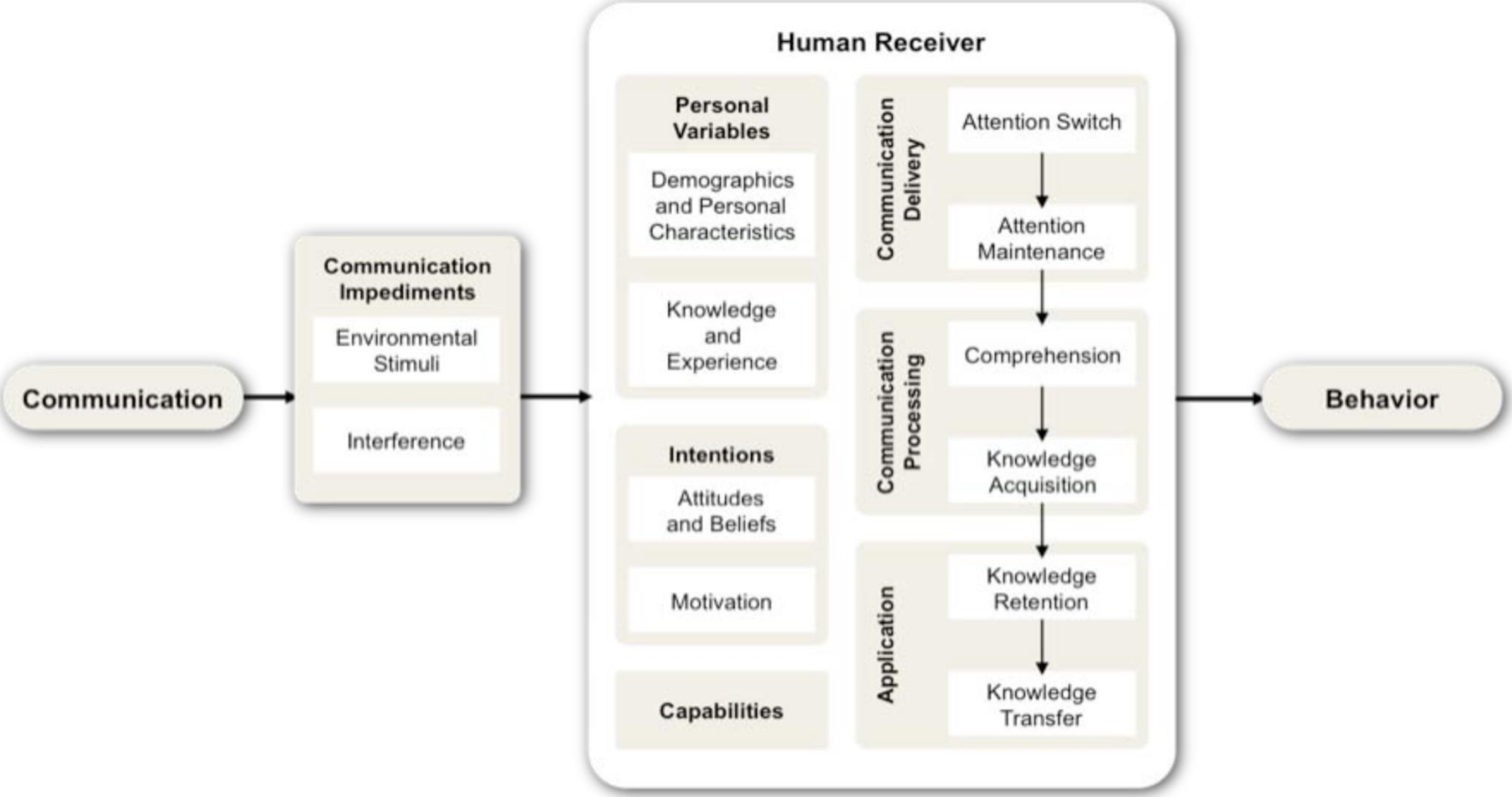
You have a new screen name! This screen name was assigned the **18+** category, which means you have unrestricted access to all AOL areas and Web sites.

AOL wants you to have safe and rewarding experiences online. So before you explore online, please take a few minutes to review a few important account safety tips. *It's a good idea to print this letter for future reference (from the File menu, select **Print**).*

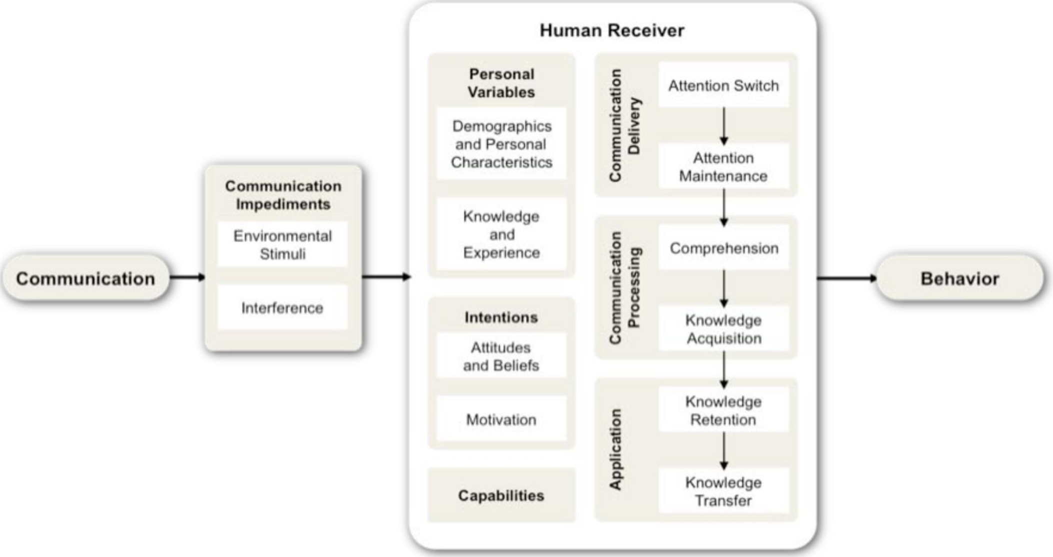
Figure 3.11: America Online responded to phishing attacks by modifying its user interface so that official AOL mail looked different than mail sent by other users. As a result, official messages could not be spoofed by outsiders or other AOL members [Garfinkel, 2005, p.199].

Anti-Phishing – Human in the Loop

- Lorrie Faith Cranor. 2008. A framework for reasoning about the human in the loop. In Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC'08), Elizabeth Churchill and Rachna Dhamija (Eds.). USENIX Association, Berkeley, CA, USA, Article 1, 15 pages.
- Wu “Wizard of Oz” Lab Study
  - Neutral information bar (domain name, registration date, hosting country): 45% spoofed
  - SSL verification tooldbar (CA, etc): 38% spoofed
  - Traffic light toolbar (red/orange/green): 33% spoofed


Communication
Communication Impediments
Environmental Stimuli
Interference
Human Receiver
Personal Variables
Demographics and Personal Characteristics
Knowledge and Experience
Intentions
Attitudes and Beliefs
Motivation
Capabilities
Communication Delivery
Attention Switch
Attention Maintenance
Communication Processing
Comprehension
Knowledge Acquisition
Application
Knowledge Retention
Knowledge Transfer
Behavior

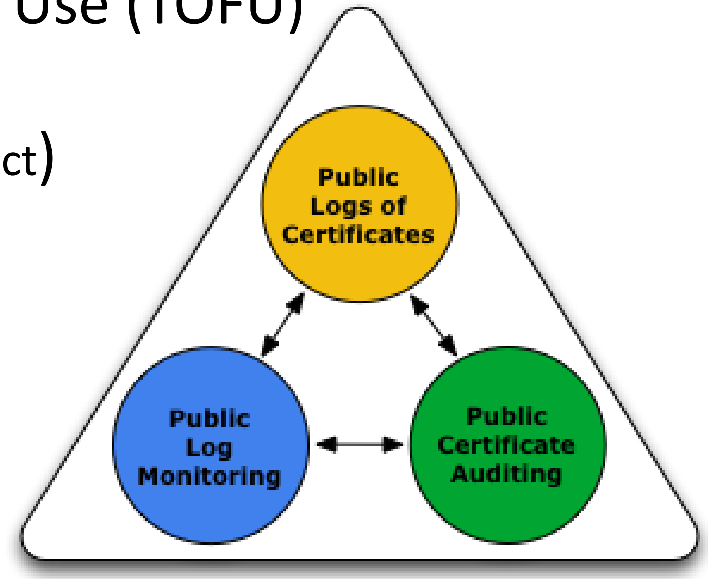
Communication



1. warnings,
2. notices,
3. status indicators,
4. training, and
5. policies.

Anti-Phishing Today

- Passive Indicators still used
  - Extended Validation Certificates (company name, contact information, ...)
  - Domain Highlighting
  - Key Continuity Managment (KCM) / Trust On First Use (TOFU)
  - Certificate Transparency
    (Image source: https://www.certificate-transparency.org/what-is-ct)



Storage

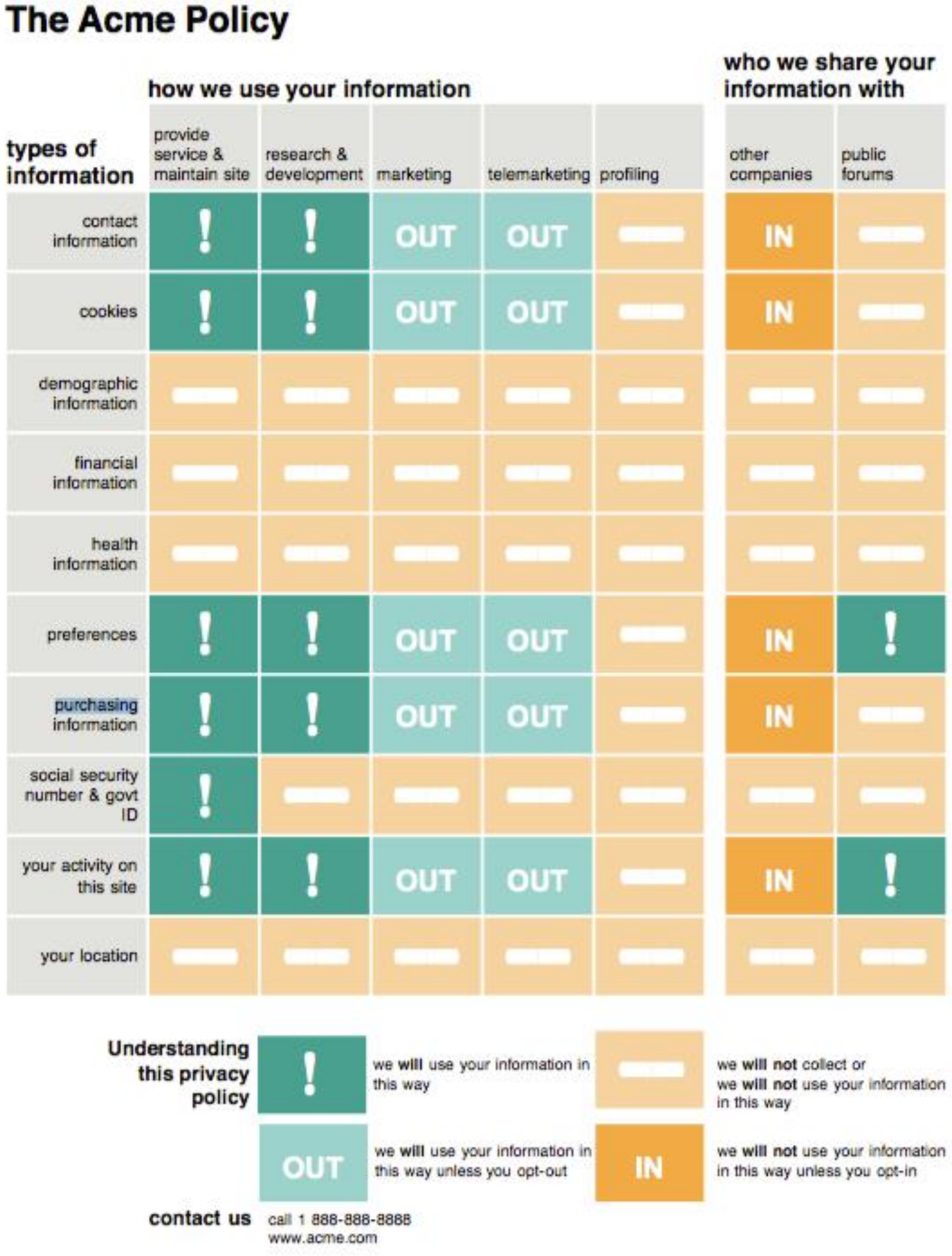
- Assured deletion and durability
- Studies show that users do not really worry.
- Modern file systems make wiping more complicated (think copy on write and SSD).

Device Pairing

- Over a secured wired connection
- Out-of-band information
    - Location-limited channels (infrared, high-frequency audio, flashing LEDs, shaking, ...)
- Comparing hashes, numbers, etc.
    - Force people to re-type them

Web Privacy

- P3P policies
  - Not widely deployed
  - Syntax errors, thus not usable
  - Machine readable form was different to human readable version
- Behavioral advertising
  - 2912 Mechanical Turk participants said they would never share personal information
  - 45 participants in a lab study had problems with selectively blocking cookies and using blocking tools



The Acme Policy

	how we use your information					who we share your information with	
types of information	provide service & maintain site	research & development	marketing	telemarketing	profiling	other companies	public forums
contact information	!	!	OUT	OUT	—	IN	—
cookies	!	!	OUT	OUT	—	IN	—
demographic information	—	—	—	—	—	—	—
financial information	—	—	—	—	—	—	—
health information	—	—	—	—	—	—	—
preferences	!	!	OUT	OUT	—	IN	!
purchasing information	!	!	OUT	OUT	—	IN	—
social security number & govt ID	!	—	—	—	—	—	—
your activity on this site	!	!	OUT	OUT	—	IN	!
your location	—	—	—	—	—	—	—

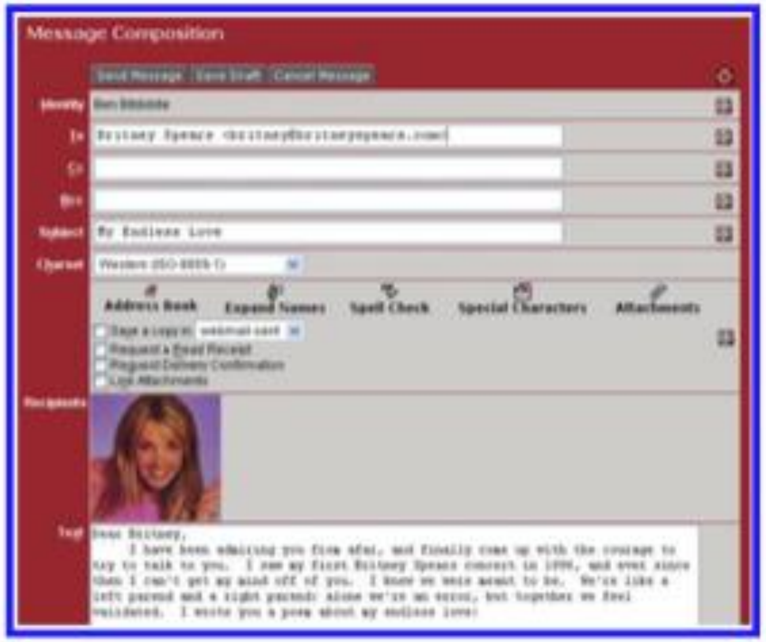
Understanding this privacy policy				
	!	we **will** use your information in this way	—	we **will not** collect or we **will not** use your information in this way
	OUT	we **will** use your information in this way unless you opt-out	IN	we **will not** use your information in this way unless you opt-in

contact us call 1 888-888-8888
www.acme.com

Figure 3.15: A privacy label. (Based on Kelley et al. [2010].)

Policy Specification and Interaction

Sending E-Mail to (too) many people



Identity: Ben Bitdiddle

To: Britney Spears <britney@britneyspears.com>

Subject: My Endless Love

Charset: Western (ISO-8859-1)

□ Save a copy in: webmail-sent
□ Request a Read Receipt
□ Request Delivery Confirmation
□ List Attachments

Dear Britney,
I have been admiring you from afar, and finally come up with the courage to try to talk to you. I saw my first Britney Spears concert in 1999, and ever since then I can't get my mind off of you. I know we were meant to be. We're like a left paren and a right paren: alone we're an error, but together we feel validated. I wrote you a poem about my endless love!

Figure 3.16: Facemail composition window. (Figure 1 from Lieberman and Miller, 2007)

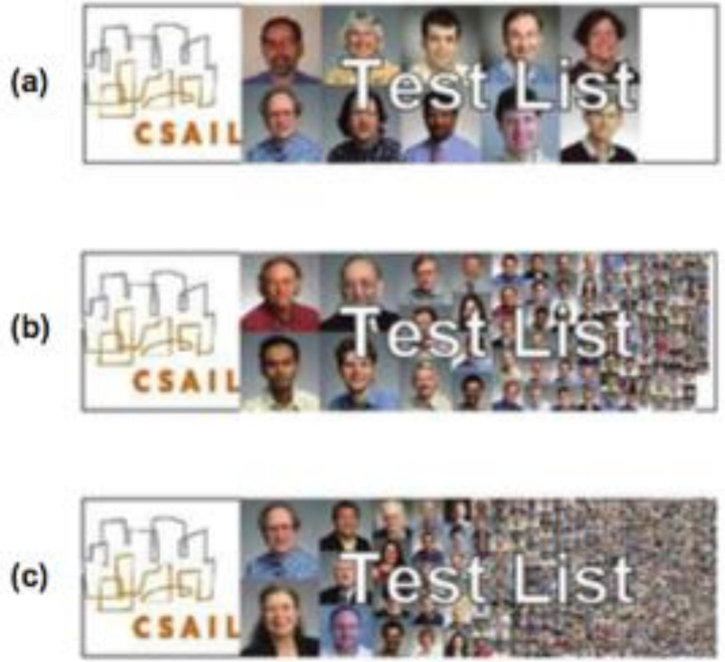


Figure 3.17: Progressive scaling grid showing (a) 10 faces, (b) 100 faces, and (c) 1,000 faces. (Figure 3 from Lieberman and Miller, 2007)

Access Control

- Make access control more visible, by incorporating policies alongside the context of use
- Simplify access control patterns and interfaces,
- Support ad-hoc and temporary sharing,
- Support real-time policy updates, and
- Support and reflect social conventions

Mobile Security and Privacy

- Location Privacy
  - Depending on **who** wants to know the location for **which reason** and **what** the current location is.
  - Create rules on how to share information. ...too complicated
  - Actively check-in (four-square) to share with friends (and Facebook)
- App Permissions
  - 83% just click yes
  - Users do not understand the language
  - In the past, users can only not use application