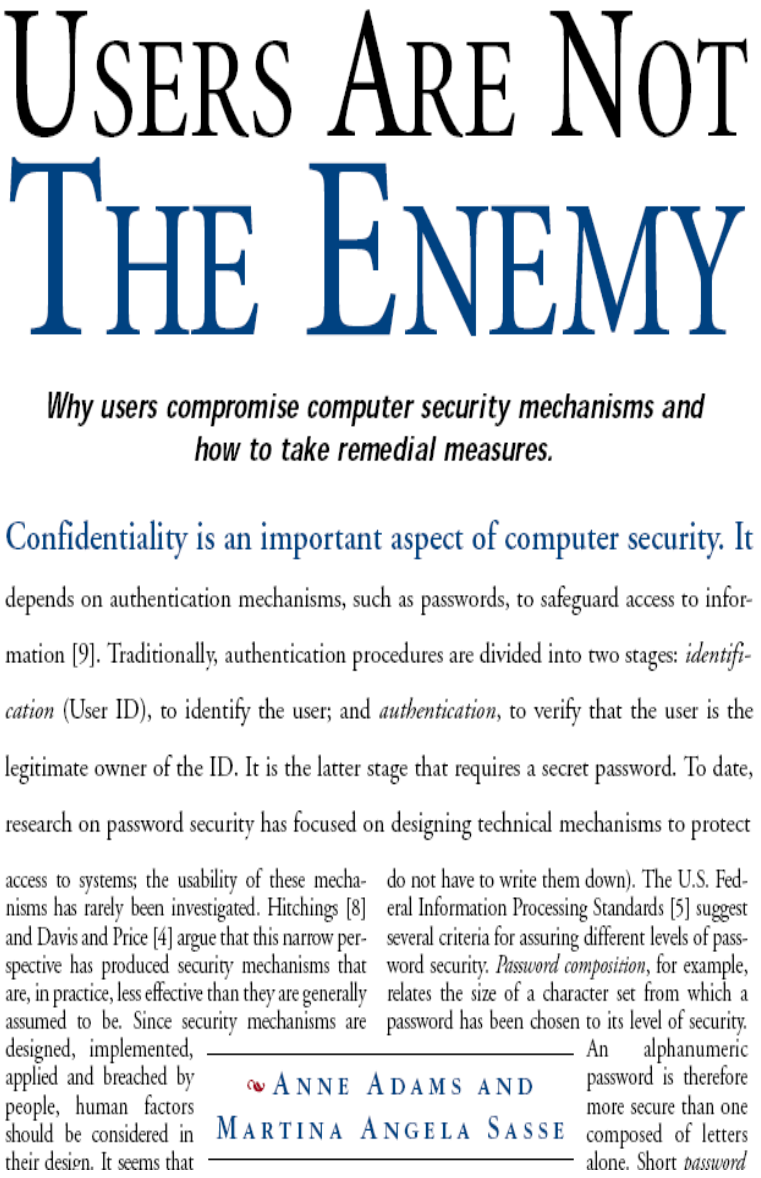
Usability and Security

Overview

- A brief history of “usable security”
- Why HCI leads to better security
- But: usable is not enough
  - The knowledge gap
  - The motivation gap
  - Considering impact on users

How I got into security

- Study on password problems BT Labs in 1996 (with Anne Adams)
- Findings:
  - Too many passwords
  - Too many password changes
  - Users don't understand risks, threats and how their behavic relates
  - State of war between users a security department



USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security. An alphanumeric password is therefore more secure than one composed of letters alone. Short *password*

ANNE ADAMS AND MARTINA ANGELA SASSE

"Why Johnny can't encrypt"

- Whitten & Tygar, *Procs USENIX 1999*
- Graphical user interface to PGP 5.0
- Even after detailed introduction, only 3 out of 12 participants could encrypt their email successfully
- Need more than a pretty face: graphical ≠ usable
- Problems:
  1. User tasks not represented in UI
  2. Misleading labels
  3. Lack of feedback

Human-Computer Interaction

general & specific characteristics

USER

SYSTEM

interacts with

to attain

GOAL

by carrying out **TASK**

interaction takes place in a

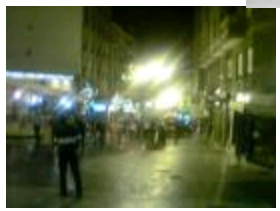
CONTEXT

physical

social

cultural

temporal



General User Characteristic: Human Memory

- Limited capacity
- Decays over time (items cannot be recalled at all or not 100% correct)
- Frequent recall improves memorability
- Unaided recall is harder than recognition
- Non-meaningful items much harder to recall than meaningful ones
- Similar items are easily confused
- Items linger - cannot “forget on demand”

Password Systems

- Require unaided recall
- Entry must be entered 100% correct
- Not meaningful (no words, names, phrases)
- Many similar items compete
  - Frequently change
  - Proliferation of items that users have to recall (banking, phones, websites)

More on knowledge-based authentication

- Most people struggle even more with PINs than with passwords
- Majority of people write down all or some of their passwords and PINs
- Passwords and PINs chosen by people are vulnerable to cracking and guessing attacks
- People re-use passwords (usually indiscriminately)

Importance of goals, tasks and performance

- *Passfaces* trial
- Good memorability, even after 3 months
- But: too slow for regular logins
- Decreased usage of system by 60%

User choices & security implications

Image Population	Female model	Male model	Typical female	Typical male
female	40%	20%	28.8%	11.3%
male	63.2%	10%	12.7%	14%

- *“In order to remember pictures for my login (after forgetting my password 4 times in a row), I needed to pick pictures I could easily remember – kind of the same pitfalls when picking a lettered password. So, I chose all pictures of beautiful women.”*
- *“I simply pick the best-looking girl on each page.”*

Quotes from Montrose & Reiter (2005)

Ethnicity bias - security implications

Population	Asian	Black	White
Asian female	52.1%	16.7%	31.3
Asian male	34.4%	21.9%	43.8%
Black male	8.3%	91.7%	0.0%
White female	18.8%	31.3%	50%
White male	17.6%	20.4%	62%

“I started by deciding to choose faces in my own race … specifically, people that looked at least a little like me. The hope was that knowing this general piece of information about all of the images in my password would make the individual faces easier to remember.”

www.gridsure.com

GrIDsure™

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

- Personal Identification Pattern
- User selects pattern from grid (min. 5 x 5)
- Numbers displayed on grid
- User reads PIN off grid displayed on personal device (phone/PDA) and enters one-time PIN into sales unit/ATM/home PC.

VIDOOP

- two-factor system using both
- a ‘soft token’ on user’s PC
- selection Vidoop image grid → access code

Jakob Nielsen's Alertbox November 26, 2000

"In future, security [and usability] will improve through biometrics such as fingerprint and retina scanning (though fingerprints don't work for some people."

BBC NEWS UK EDITION

Last Updated: Wednesday, 17 September, 2003, 08:38 GMT 09

E-mail this to a friend Printable version

Eye scan school opens doors

A £14m Sunderland secondary school opens its doors to pupils on Wednesday, after a delay of a week and a half.

The Venerable Bede Church of England school should have opened on 8 September but building works also overshot a second opening date last Friday.

The system will be used for ordering school dinners

Staff and governors at the so-called "super school" have said that the best is worth waiting for with a building and facilities fit for the 21st century.

BBC NEWS UK EDITION

Last Updated: Monday, 13 September, 2004, 15:29 GMT 16:29

E-mail this to a friend Printable version

Eye scanner project is scrapped

A Wearside school which became the first in Europe to use a futuristic eye-scanner has scrapped the scheme because it was too slow.

The eye scanner has been scrapped for being too slow

Venerable Bede Church of England School in Ryhope, Sunderland, introduced the hi-tech system to take away the stigma felt by pupils entitled to free meals.

The scanner was able to identify pupils anonymously by taking a picture of their eyes.

But the scheme has now been replaced by swipe cards because it was too slow.

"We were aiming for it to scan 12 pupils a minute, but it was only managing 5 so has been temporarily suspended as we do not want pupils' meals getting cold while they wait in the queue."

Performance requirements need to be understood & accommodated

Other issues with biometrics - exclusion? Failure-to-enrol rates

	Face	Iris	Finger
Quota	0.15%	12.30%	0.69%
Disabled	2.73%	39%	3.91%

UKPS (UK Passport Service) enrolment trial 2004

FAR & FRR

- FAR (False Acceptance Rate)
  - accepting user who is not registered
  - mistaking one registered user for another
  - High security: FAR of .01% acceptable
- FRR (False Rejection Rate)
- – rejecting legitimate user
- High FRRs reduce usability, high FARs reduce security
  - customer-based applications tend to raise FAR

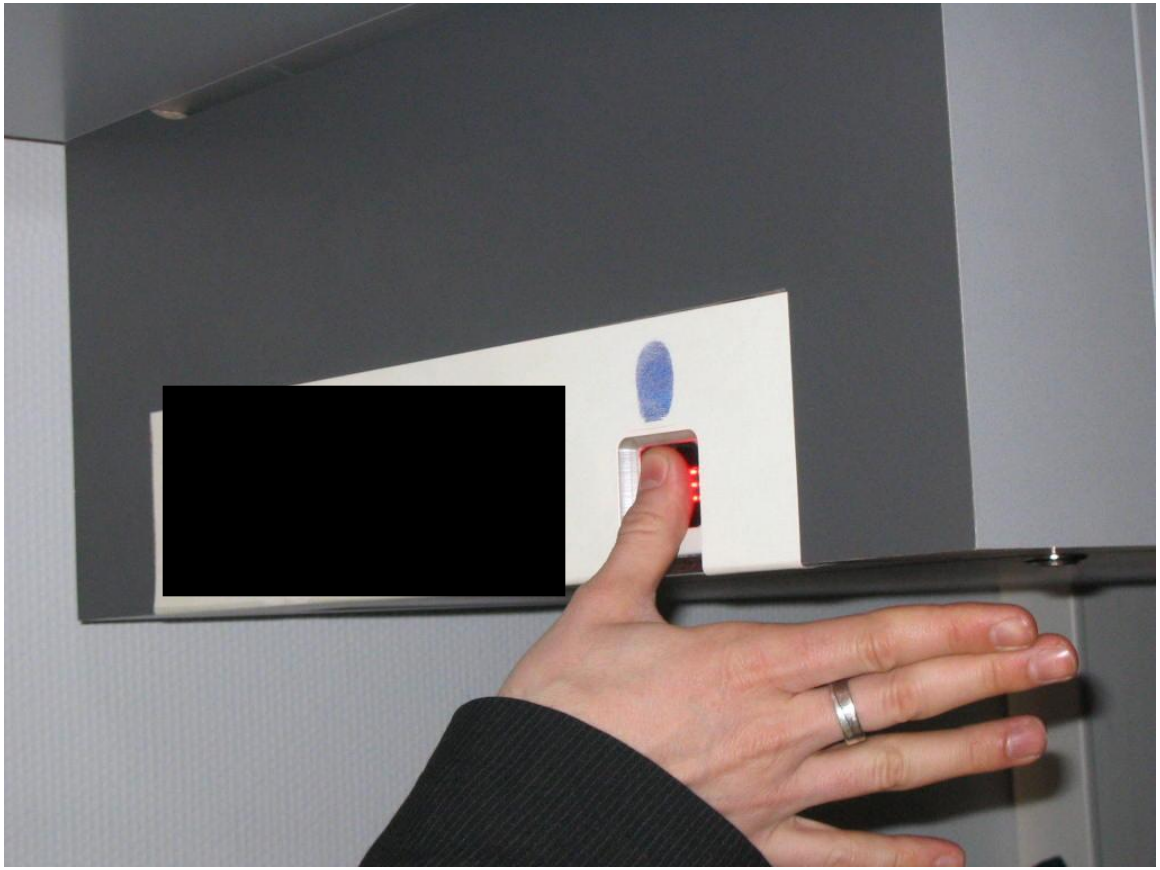
FRR in UKPS enrolment trial

	Face	Iris	Finger
Quota Time:	30.82% *39 sec*	1.75% *58 sec*	11.70% 1 min 13 sec
Disabled Time:	51.57% *1 min 3 sec*	8.22% *1 min 18 sec*	16.35% *1 min 20 sec*

Example: BKA face recognition trial

- Railway station with 20,000 passengers/day
- 2 month trial of 3 systems
- 200 people on watch list, who passed through every day, making no effort to conceal their identity
- FAR fixed at .1% (= 23 false alarms/day)
- Best performing system at under most favourable detected caught 60% (down to 20%)

Which finger?



Finger position?

Focussing

Height adjustment

… but users may not realise this

… or be reluctant to
touch equipment,
or think it takes too long

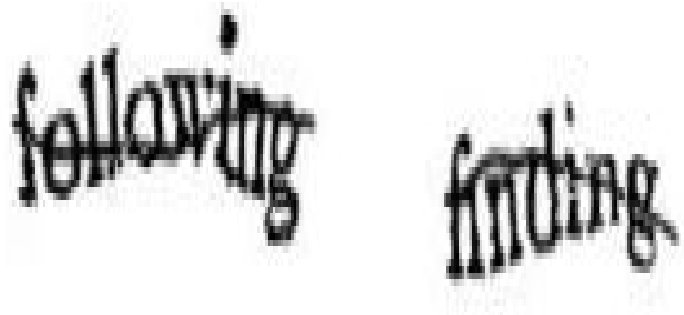
Distance

“Neutral expression”

Failure to consider user goals

- Security is often designed to “defend the system”, without considering user goals
- Examples:
  - Chip and PIN
  - Phishing
  - CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart)
- Result:
  - Reduced security
  - Increased cost
  - Reduced business

Early CAPTCHAs such as these, generated by the EZ-Gimpy program, were used on Yahoo. However, technology was developed to read this type of CAPTCHA



A modern CAPTCHA. Rather than attempting to create a distorted background and high levels of warping on the text, this CAPTCHA focuses on making segmentation difficult by adding an angled line.

Another way to make segmentation difficult. Crowded symbols can be easily read by humans but can't be segmented by bots.

Impact of security on lived experience

- Consequences of failure: blocking access of legitimate users is like slamming a door in their face
  - What is the impact on lived experience – e.g. not paying your bill on time, not catching your plane?
  - Creates negative/adversarial stance, when you want to engage and motivate users
- Can put people off using services
  - introduction of CAPTCHA reduced number of genuine subscribers by 50%
  - Accessibility – people may not get advantages of services they don't understand/trust

Security Awareness, Education & Training

- “Educating users” is often seen as way forward (cheaper than designing usable security)
- But: most security training is not effective
  - not targeted at specific user needs & responsibilities
  - dull: little more than repeating policies (not improving user understanding or skills)
  - cheap: delivered on-line to save costs
- There is a significant knowledge & skills gap - not just among users - system developers and administrators

Conclusions

- Most people like to believe that security is provided through technology.
- *“If you believe that, you don’t understand security or technology.”* Bruce Schneier
- Security isn’t that special – application of usability/design knowledge and methods solves most problems.
- Do not focus on UIs to security tools – the big problems are in security requirements, job design and user involvement