

Introduction

HCI & HCISec

Mike Just, Heriot-Watt University
COINS Summer School on Auth Ecosystems

31 July 2016

About Me

- ▶ Associate Professor, School of Mathematical & Computer Sciences, Heriot-Watt University, Edinburgh, UK
- ▶ “I use HCI & machine learning to improve computer security”
- ▶ Career path
 - ▶ PhD in applied cryptography (1998)
 - ▶ Security architect in industry (4 years)
 - ▶ Security design and policy in public sector (6 years)
 - ▶ Academic (2008 – present)
- ▶ My path to usable security ...

My University

- ▶ Heriot-Watt University
 - ▶ Edinburgh, UK (Scotland). Also Dubai, Malaysia campuses
 - ▶ ~5000 students in Edinburgh. Focus on Eng, Maths, and CS
 - ▶ Ranking: ~20th (of ~120) in UK; ~3rd (of 15) in Scotland
 - ▶ University partners in Scotland:
Aberdeen, Edinburgh, Glasgow, St. Andrews, . . .
- ▶ Heriot-Watt Computer Science
 - ▶ About 40 permanent academic staff (and growing)
 - ▶ First computer science degree programme in Scotland (1966)
 - ▶ Some research areas: machine learning, natural language processing, robotics, HRI, HCI, formal methods, programming languages, computer security

Today's lectures

- ▶ Usable security (HCI_{Sec})
 - ▶ Designing and evaluating security techniques that are usable (efficient, effective, satisfaction)
 - ▶ “Usable” as a means to improve security
- ▶ Authentication
 - ▶ I find this topic interesting
 - ▶ Though, I try to look at practical solutions
- ▶ Today
 - ▶ Investigate the usability and security of some existing techniques: passwords, challenge questions, multiple factors
 - ▶ Behavioural authentication: the present and future of authentication
 - ▶ Much of the work discussed today is based on my own research

Why Human-Computer Interaction? (1)

- ▶ Technical skills alone **do not suffice** for building a computer system, much less a secure computer system
- ▶ Computers are essentially a medium through which humans perform tasks. The interaction between humans and computers then becomes important
 - ▶ Hence the field of **Human-Computer Interaction (HCI)**
- ▶ And HCI is as important to security as it is to the broader computer science

Human versus Computer?



Copyright 2003 Randy Glasbergen. www.glasbergen.com

Causes of security failure

There are three primary causes of security failure:

1. Attackers

- ▶ With no attackers, there'd be no (intentional) security failures
- ▶ We'd still have unintentional failures though

2. System complexity

- ▶ Complexity increases the likelihood of vulnerabilities
- ▶ E.g., millions of lines of code, and complex interfaces and processes lead to likely errors

3. Human factors

- ▶ Humans make mistakes, have limited computational abilities, misunderstand instructions, are lazy, have limited memory, etc.
- ▶ Each can contribute to a security failure, especially if security is viewed as a secondary task (which it often is)

Why Human-Computer Interaction? (2)

- ▶ Psychology gives us the tools to study human behaviour
 - ▶ Existing knowledge regarding humans and their behaviour
 - ▶ Methods for evaluating further, dynamic situations
- ▶ It allows us to ask (and hopefully answer) questions such as
 - ▶ *“How do users behave, and why?”*
 - ▶ And sometimes even, *“How do attackers behave, and why?”*
- ▶ More importantly, it helps us understand the tricky balance between security and human behaviour
 - ▶ How can we design systems to meet user and security needs?
 - ▶ Does security technology place too much demand upon users?
 - ▶ Or, are users to blame for our security problems?

State of the Nation

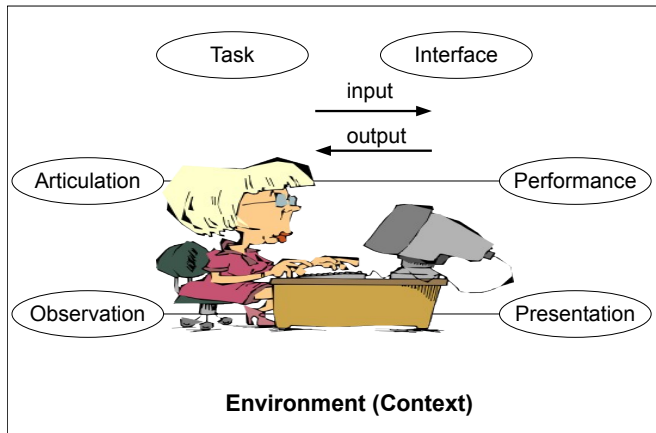
- ▶ Many security systems are not usable
 - ▶ Decrease productivity (obstacles to task completion)
 - ▶ Promote insecure behaviour (e.g., writing down passwords)
- ▶ Security techniques are not widely used
 - ▶ Not needed?
 - ▶ Too complicated to use or implement?
 - ▶ Benefits not well understood?
 - ▶ Viewed as an obstacle to productivity?

Human-Computer Interaction (HCI)

Human-computer interaction is a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them. [ACM]

- ▶ Earlier fields of Human Factors & Ergonomics
 - ▶ More stress on physical issues and optimising work processes
- ▶ User Interface Design
 - ▶ Focus on interface (and ignore deeper functionality)
 - ▶ *Usability Engineering* focuses on design and implementation
- ▶ User/Human Centred Design
 - ▶ Approach to software engineering with user focus at all stages
 - ▶ Participatory design explicitly includes users in design process
- ▶ Interaction Design
 - ▶ More emphasis on cognitive/experiential factors

The Environment



The Environment - User Characteristics

- ▶ Physical
 - ▶ Characteristics and limitations of the human body
 - ▶ Quality of characteristics varies, e.g., biometrics
 - ▶ Ageing and illness make some tasks difficult, or at least time consuming
 - ▶ Accessibility can be a major consideration
- ▶ Mental
 - ▶ Memory
 - ▶ Perceptions
 - ▶ Attitudes
 - ▶ Beliefs
 - ▶ People often look for the path of least resistance (often to reduce complexity and mental workload)

The Environment - Context

- ▶ Physical
 - ▶ Atmosphere
 - ▶ Climate
 - ▶ Lighting
 - ▶ Noise
 - ▶ Desk, chair, desktop
 - ▶ Mobile versus fixed
- ▶ Social
 - ▶ Private, semi-private, public
 - ▶ Social norms regarding acceptable user behaviour
 - ▶ Organizational culture, e.g., professional behaviour

The Environment - Tasks

- ▶ Humans are goal-oriented
- ▶ Evidenced by their behaviour regarding completion of tasks
- ▶ Security is often an external task to their goals
- ▶ Integration becomes a key part of design
 - ▶ Time required
 - ▶ Number of interactions required

Design Rules for HCI

- ▶ Over the years, many have tried to characterize *rules* for design with HCI in mind
- ▶ Useful for new design, but also for critical analysis of existing designs
- ▶ Shneiderman's 8 Golden Rules (1987)
 1. Strive for consistency
 2. Enable frequent users to use shortcuts
 3. Offer informative feedback
 4. Design dialogs to yield closure
 5. Offer error prevention and simple error
 6. Permit easy reversal of actions
 7. Support internal locus of control
 8. Reduce short-term memory load

Design Rules for HCI (2)

Norman's 7 Principles (1988)

- ▶ Use both knowledge in the world and knowledge in the head
- ▶ Simplify the structure of tasks
- ▶ Make things visible
- ▶ Get the mappings right
- ▶ Exploit the power of constraints, both natural and artificial
- ▶ Design for error
- ▶ When all else fails, standardise

Nielsen's 10 Usability Heuristics (1994)

- ▶ Visibility of system status
- ▶ Match systems to the real world
- ▶ User control and freedom
- ▶ Consistency and standards
- ▶ Help users recognize, diagnose, and recover from errors
- ▶ Error prevention
- ▶ Recognition rather than recall
- ▶ Flexibility and efficiency of use
- ▶ Aesthetic and minimalist design
- ▶ Help and documentation

Design Rules for HCI (3)

For our purpose (security), a number of principles stand out

1. Enable (frequent) users to use shortcuts
2. Offer informative feedback
3. Help users recognize, diagnose and recover from errors
4. Permit easy reversal of actions
5. Allow users to minimize memory load
6. Make things (e.g., choices) visible
7. Offer help and documentation

Design Rules for HCI (3)

For our purpose (security), a number of principles stand out

1. Enable (frequent) users to use shortcuts
2. Offer informative feedback
3. Help users recognize, diagnose and recover from errors
4. Permit easy reversal of actions
5. Allow users to minimize memory load
6. Make things (e.g., choices) visible
7. Offer help and documentation

I'll soon ask you to perform a short exercise using these principles.

Evaluating Designs

- ▶ There are many dimensions to evaluating a system with regard to human interaction
- ▶ These dimensions can be classified as follows:
 - ▶ **Who** is giving the feedback? Design expert? Fellow programmer? A typical user or member of a target user group? One person or a significant proportion of users?
 - ▶ **When** are you getting this feedback? On an early prototype or an established product?
 - ▶ **How** has this evaluation been arrived at? Is it by comparison to some guidelines, or from a simulated walkthrough? Is it from use in a realistic context ('ecological validity')?
 - ▶ **What** has been used as a measure? Quantitative (e.g., time to complete task, error rate) or qualitative (e.g., ease-of-use ratings)? Compared to recommendations or alternatives? Consistency?

Evaluation by Designers (1)

- ▶ Interface designers can apply a set of explicit design guidelines, where ratings can be given against each guideline, e.g., on a 0-4 scale (a *heuristic evaluation*)
 - ▶ Enable (frequent) users to use shortcuts
 - ▶ Offer informative feedback
 - ▶ Help users recognize, diagnose and recover from errors
 - ▶ Permit easy reversal of actions
 - ▶ Allow users to minimize memory load
 - ▶ Make things (e.g., choices) visible
 - ▶ Offer help and documentation
- ▶ Design guidelines for security might be customized from these.

Evaluation by Designers (1)

- ▶ Interface designers can apply a set of explicit design guidelines, where ratings can be given against each guideline, e.g., on a 0-4 scale (a *heuristic evaluation*)
 - ▶ Enable (frequent) users to use shortcuts
 - ▶ Offer informative feedback
 - ▶ Help users recognize, diagnose and recover from errors
 - ▶ Permit easy reversal of actions
 - ▶ Allow users to minimize memory load
 - ▶ Make things (e.g., choices) visible
 - ▶ Offer help and documentation
- ▶ Design guidelines for security might be customized from these.
- ▶ You'll use a heuristic evaluation for a short exercise

Evaluation by Designers (2)

- ▶ A *cognitive walkthrough* can also be used to step through an interaction sequence from the user's perspective
- ▶ It can be organized around steps of task execution
 1. Goal
 2. Planning
 3. Action specification
 4. Action execution
 5. Perception of outcome
 6. Interpretation of outcome
 7. Evaluation of outcome

Evaluation by Designers (3)

A cognitive walkthrough *form* might look as follows

1. Description of user's immediate goals
2. (First/next) action user should take
 - ▶ Is it obvious that action is available? Why or why not?
 - ▶ Is it obvious that action corresponds to user goal?
3. How will user access description of action?
 - ▶ Problem with accessing? Why or why not?
4. How will user associate description with command?
5. All other available commands less appropriate?
6. How will user execute command?
7. Is there time for user to act before timeout?
8. After execution, is progress towards goal obvious?

Evaluation During Use

1. Cooperative Evaluation

- ▶ User carries out task with direct feedback to/from evaluator
- ▶ Creates dialogue and can learn a lot from small number of users
- ▶ But high effort, and hard to analyse results

2. Ethnographic Studies

- ▶ Discrete observation, ideally in a “normal use” situation
- ▶ Can get a lot of data, especially on “mundane functions”
- ▶ But high effort, and hard to analyse results

3. Automated Evaluation

- ▶ Controlled environment with automated analysis
- ▶ Must have good idea of what data to capture beforehand
- ▶ Hard to deal with surprises

Evaluation After Use

1. Post-task walkthrough
 - ▶ Combined co-operative and ethnographic
 - ▶ Participants recorded and ask about performance afterwards
 - ▶ Sometimes called a “re-enactment protocol”
2. Interviews
 - ▶ Good for revealing unanticipated problems
 - ▶ Can also be used early in process
3. Surveys and questionnaires
 - ▶ Can ask of participant background and/or attitudes
 - ▶ Can be open-ended, ratings-based, multiple choice
 - ▶ Can also be used earlier in process

Evaluation and Security

- ▶ Many of the evaluation techniques can be directly applied to a evaluating a security system
- ▶ Security evaluation can also introduce some challenges
 - ▶ Ethical challenges with collecting real data, e.g., passwords
 - ▶ Having users participate *realistically* so that experiment/study results are *ecologically valid*
- ▶ Though it is possible to deal with the ethical challenge
 - ▶ We'll see this later with challenge questions

Usability and Security (1)

[S]ystems security is one of the last areas in IT in which user-centred design and user training are not regarded as essential

[H]ackers pay more attention to the human link in the security chain than security designers do.

[Adams and Sasse, 1999] (And still true today!)

Usability and Security (2)

- ▶ How is HCI used with security today?
 - ▶ Critical analysis of current security techniques
 - ▶ Gathering and understanding context (e.g., user needs and requirements)
 - ▶ Design of new security techniques (e.g., iterative co-design with users)
 - ▶ Evaluation of proposed techniques (e.g., lab studies, field studies)
- ▶ What sort of evidence is gathered?
 - ▶ Qualitative: Design input, explanations of behaviour
 - ▶ Quantitative: Metrics for task duration, success, user perceptions

Usable security examples

- ▶ Let's start by looking at some examples of usable security issues, and consider some possible solutions
- ▶ We'll look at several examples
 - ▶ Biometrics authentication
 - ▶ File encryption
 - ▶ Web security

Biometrics

Physical

- ▶ Fingerprint
- ▶ Finger / Palm vein
- ▶ Hand geometry
- ▶ Iris
- ▶ Retina
- ▶ Face recognition
- ▶ Earshape

Behavioural

- ▶ Voice print
- ▶ Dynamic signature recognition (DSR)
- ▶ Typing pattern
- ▶ Gait recognition
- ▶ Heart rate analysis

Some Considerations

- ▶ Performance
 - ▶ E.g., storage of full images versus templates
- ▶ Usability
 - ▶ E.g., failure to Enrol/Acquire
- ▶ Security
 - ▶ False Acceptance versus False Rejection
- ▶ User Acceptance

Fingerprints I

- ▶ Used in various authentication applications
 - ▶ Doors, PCs/laptops, US visit programme
- ▶ Failures to Enrol/Acquire
 - ▶ Worn down fingerprints, callouses (manual work, chemicals, sports, age), deformation, arthritis
- ▶ Usability issues
 - ▶ Which finger?
 - ▶ Where to position on sensor?
 - ▶ Which part of finger?
- ▶ User acceptance issues
 - ▶ Hygiene!, association with forensics/criminals, finger chopped off
- ▶ Security
 - ▶ Recovery from glasses, etc.,
 - ▶ Then creation of gelatine/silicon prints (“gummy bear attack”)

Fingerprint Examples

BBC NEWS WORLD EDITION

Last Updated: Thursday, 31 March, 2005, 10:37 GMT 11:37 UK

[E-mail this to a friend](#)

[Printable version](#)

Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.

The car, a Mercedes S-class, was protected by a fingerprint recognition system.

Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb.

The gang, armed with long machetes, demanded the keys to his car.

It is worth around \$75,000 second-hand on the local market, where prices are high because of import duties.



Facial Scan

- ▶ Used in various authentication applications
 - ▶ E.g., passports
- ▶ Usability
 - ▶ Where to stand, stare?
 - ▶ Neutral expression
 - ▶ UK passport trial had a false rejection rate of 30% for face recognition
- ▶ User acceptance issues
 - ▶ Covert identification
 - ▶ Surveillance/track (e.g., for direct marketing purposes)
- ▶ Security
 - ▶ Using a photo or video of a person
 - ▶ Using a mask (á lá Mission Impossible)

Facial Scan – Usability



Iris/Retina Scans

- ▶ Used in various authentication applications
 - ▶ Passports, schools
- ▶ Usability issues
 - ▶ Distance adjustment, positioning
 - ▶ Glasses, contact lenses
- ▶ User acceptance issues
 - ▶ Risk to health, e.g., damage to eyes, trigger epilepsy
 - ▶ Covert medical diagnosis
- ▶ Security
 - ▶ Pictures of eyes on glasses
 - ▶ Contact lenses

Iris Scan – Usability (1)



Iris scan example I

- ▶ In 2003, an English school decided to introduce biometrics authentication as part of a free school lunch program
- ▶ The proposal was intended to remove the stigma felt by pupils entitled to the meals by identifying them anonymously
- ▶ The idea was also part of a push to build a school for the “21st century”
- ▶ The school hoped to be able to scan 12 pupils a minute

Iris scan example II

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.

Iris scan example III

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.

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 eye scanner has been scrapped for being too slow

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

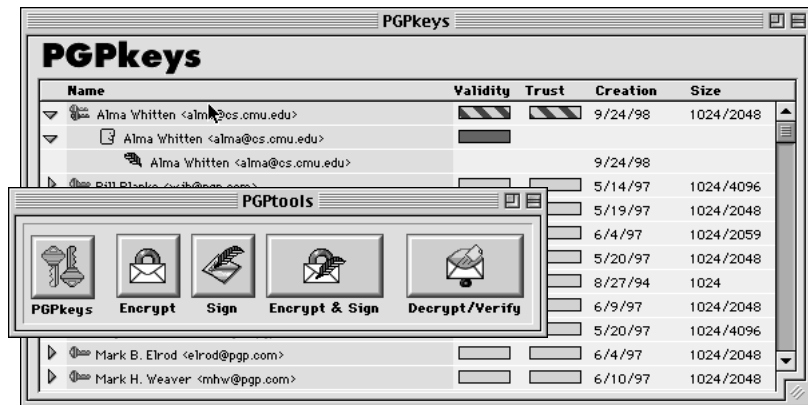
But the scheme has now been replaced by swipe cards because it was too slow.

The school returned to using a swipe card system

Iris scan example IV

- ▶ In reality, only 5 pupils a minute were scanned (not 12)
- ▶ The project planning had not thoroughly considered the *task* of biometrics authentication
- ▶ It had only considered the time for biometrics capture, and not
 - ▶ Presentation at the machine
 - ▶ Setting handbag aside, removing jacket, etc.
 - ▶ Finding token (if used)
 - ▶ Positioning oneself
 - ▶ Waiting for image to be captured and matched
 - ▶ Wait for confirmation of completion
 - ▶ Collecting belongings and walking away
 - ▶ Failed attempts

File encryption I

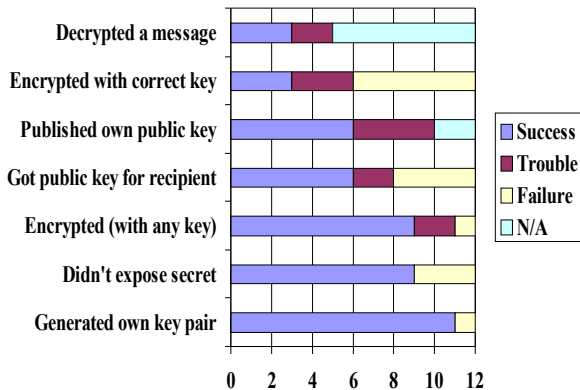


“significantly improved graphical user interface makes complex mathematical cryptography accessible to novice computer users”

File encryption II

- ▶ Local file encryption can be done “easily”, due to its transparency
- ▶ However, end-to-end application level confidentiality and integrity is more challenging for users
- ▶ Why?
 - ▶ Concepts such as *keys*, *encryption* and *signing* can be difficult to match to people’s *mental models*
- ▶ The result, for studies of GPG/PGP encryption
 - ▶ Users struggle to decrypt data
 - ▶ Users struggle to encrypt data for others
 - ▶ Users struggle to create and share keys

File encryption III



Web security

- ▶ How do you know that you're visiting a legitimate web page?
- ▶ There are various reasons that a web page might not be trusted
 - ▶ Certificate error (expiry, wrong domain, etc.)
 - ▶ Suspected phishing or malware site
- ▶ *Passive warnings* can signal a user that a web page might not be trusted, though the user has to notice the warning (and know how to act on it)
 - ▶ The user can click for more information

Web security – passive warnings – red

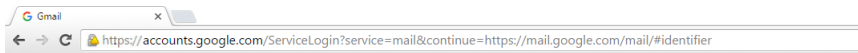


Google
UK

Google Search


I'm Feeling Lucky

Web security – passive warnings – yellow



One account. All of Google.

Sign in to continue to Gmail



[Need help?](#)

Web security – passive warnings – green

Log in to Digital Banking

The Royal Bank of Scotland Group Plc [GB] https://www.rbsdigital.com/default.aspx?refererid=63D05112CF3C40257D18D0...

Personal Private Business Corporate International

Royal Bank of Scotland Products Support Life Moments

Digital Banking Services

Digital banking Credit card services

Welcome to Digital Banking

Customer number > [Forgotten any of your log in details?](#)

This is your date of birth (ddmmyy) followed by your unique number which identifies you to the bank.

Remember me. We don't recommend storing data on a shared computer.

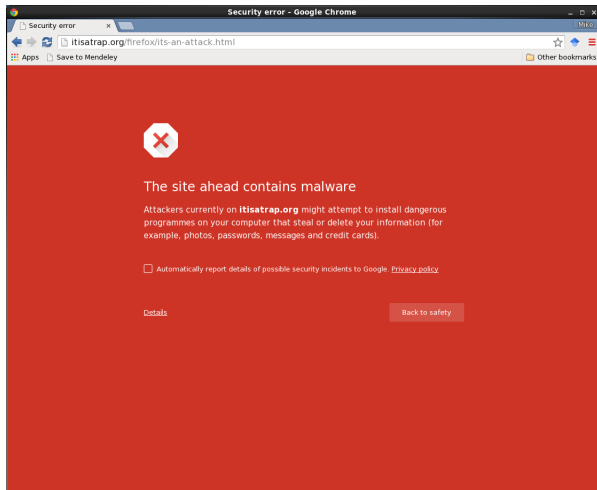
> [Tell me more about this feature](#)

Log in

Web security – passive warnings

- ▶ Do people know what the different colours mean?
- ▶ What would you do in each situation?
 - ▶ Continue ahead to the page!
 - ▶ Find out more information
 - ▶ Stop and try another page
 - ▶ Go for lunch
- ▶ Do people notice such warnings?
- ▶ In reality, most people don't notice passive warnings

Web security – active warnings I



Web security – active warnings II

- ▶ *Active warnings* require notice to be taken
 - ▶ They require an action from the user
 - ▶ They also interrupt the primary task
- ▶ In terms of security protection, they can protect a user from continuing to a page
- ▶ However, what should the user do next?
 - ▶ If the users knows/believes the page to be safe, they can continue (albeit, after a few clicks)
 - ▶ If the user has indeed been protected from a security attack, what do they do next?

Web security – active warnings III

Your web browser thinks this is a phishing web site. Do you want to go there anyway?

You are trying to go to evilsite.com. Do you really want to go there or would you rather go to yourbank.com?

Which option aids the continuation of the primary task?
Which options hinders it?

Short exercise

- ▶ Visit a website of your choice and examine the process for either **account registration** or **account login**
- ▶ Perform a **heuristic evaluation** in which you give a **ternary rating (yes; maybe; no)** as to whether the website registration or login meets the following principles
 - ▶ Enable (frequent) users to use shortcuts
 - ▶ Offer informative feedback
 - ▶ Help users recognize, diagnose and recover from errors
 - ▶ Permit easy reversal of actions
 - ▶ Allow users to minimize memory load
 - ▶ Make things (e.g., choices) visible
 - ▶ Offer help and documentation