### Usable Security - Human Computer Interaction Basic

1. Human-Computer Interaction is the study of: How people interact with technology  
  
2. Imagine you are analyzing the usability of a banking website. The Examples of good task can be

* Check your savings account balance.
* Transfer $5 from checking to savings.

3. The measures of Usability are as follows:

* Speed
* Efficiency
* User Preference
* Memorability
* Learnability

4. Chunking: Aggregating several pieces of information into coherent groups to make them easier to remember.  
  
5. The following are examples of conventions that improve mental models

* Using a qwerty keyboard on a new device
* Color coding warnings in red and alerts in yellow
* Putting options to create a new file and save a file under a "File" menu in the upper left of the application.

6. The people included in an HCI study might include:

* Users who have Technology Embedded in Wearable Items
* Mobile Device Users
* Desktop or Laptop Computer Users

7. Three important things that have to be understood in HCI are:

* Users
* Tasks
* Contexts

8. How should users be considered within a security system?

* They are an integral part of security and should be considered part of the system from the beginning.

9. Factors to consider in designing usable interfaces:

* The users' expertise and experience with computers

**Usable Security - Design**

1. The cycle of the iterative design process

* Requirements
* Design
* Developments
* Testing

2. The difference between system centered design and user centered design:

* System centered design is focused on what is easy to build on a platform while user centered design is focused on user needs and context

3. Good ways to incorporate user-centered design in the design of security systems can be

* Designing security around user tasks
* Designing security based on the user's environment and work context

4. NOT Good ways to incorporate user-centered design in the design of security systems

* Designing security based on what experts believe is best.

5. When designing error messages, followings are important factors to keep in mind for usability

* Use language that users will understand
* Make the most secure options part of the user's natural task
* Provide users with clear exits to get out of a security warning

6. If you were designing security for the entrance to a secure facility, which of the following should you consider?

* How often users enter and exit
* What tasks the users are in the middle of when they need to access the area.

7. Following are disadvantages of Personas:

* Too many personas can be difficult to create and manage.
* A diverse audience may be difficult to represent with a normal-sized set of personas

8. The advantages of low-fidelity (e.g. paper) prototypes:

* They can be created quickly and cheaply
* Any team member can create one, regardless of programming skills

9. Following are present in good interface design:

* Easy to recover from errors
* Minimal training needed for a person to use the system
* Relies on common interaction techniques for familiarity

10. Compute the efficiency of the underlying algorithms: is NOT an important part of the design process  
11. Following is an important part of the design process:

* Prepare a prototype
* Consider usability guidelines
* Solicit user input

12. In participatory design and co-design: Average users have equal standing with designers  
13. In participatory design and co-design, the following are not true

* Managers convey input from users to designers
* Users design the system on their own based on a list of constraints provided by designers
* Designers brainstorm and create prototypes after asking potential users questions

### Usable Security - Evaluation

1. Heuristic Evaluation: Analyzing a system according to a set of guidelines for good usability.  
2. The goal of Usable Security

* To measure and describe usability of a system for given tasks

3. The following are NOT the goal of Usable Security:

* To develop new measures of usability
* To test the security of a system
* To study the theoretical aspects of usability

4. What is the goal of A/B testing?

* To compare the performance two (or more) interface variations

5 If we ran an experiment to test if password logins were faster than a voice recognition authentication system, what would be required to show passwords were faster?

.

Statistical tests showed that the password group logged in significantly faster than the voice-recognition group  
6. What would you do when running a controlled experiment to evaluate an interface?

* Have some people try using the control interface while other people try using the experimental interface
* Have each person in the experiment try both interfaces.
* Provide users with training and instructions on how to use the control and experimental interfaces

7. What not to do

* Select average users to test the control interface and expert users to test the experimental interface.

8. Qualitative evaluation is intended to: Understand user experiences and reactions to a design  
9. Qualitative evaluation is not intended to:

* Count the number of errors a user makes when using the system
* Time how long it takes a user to complete a task
* Measure how well a user remembers the steps required to complete a task

10. Following are standard observation method:

* Silent Observer
* Constructive Interaction
* Think Aloud

11. Why do we conduct usability studies on systems that have already been designed?  
It is because Despite their best efforts, designer and developers cannot know exactly how users will interact with their system. A usability study will find previously uncovered errors.

### Usable Security - Guidelines

1. Principle of least privilege: A system should be able to access only the information it needs to perform its functions.  
2. A design guideline for creating usable secure systems is to make the most secure way to complete a task the easiest way to complete the task.  
3. Users should be aware of what authority they hold, what authority they have granted, and what the implications are for security decisions.  
4. The more usable a system is, the more secure it is because usable systems help users make good security decisions and easily choose the most secure actions.   
5. Guidelines for creating usable security systems:

* Create interfaces that make it clear what software the user is interacting with and providing information to.
* Make sure users know what authority they hold
* Make sure that users know what authority they have granted and what that means for security decisions

6. If you are warning users about a security problem that has been detected, the best message to show them:

* A message that alerts them to the error and makes the most obvious option the one that stops the user from proceeding. A small link is given to ignore the warning and proceed.

7. What should be considered In a system where a person can grant authority to others to his or her own access resources

* The interface should help users be aware of what authority they have granted in the past
* The easiest way to do a task should require the most minimal granting of authority
* Users should be able to reduce the authority granted to others

8. Which guideline is violated when an interface does not make capitalization differences unambiguous (e.g. a lower case "L" and capital "i" appear to be the same thing)

* Make it easy to see the differences between objects and actions that could be confused.

### Usable Security - Authentication

1. Fingerprint recognition is generally faster than password entry for authentication.  
   
2. Following are measures of usability for authentication systems:

* Speed
* How easy it is to learn
* Likelihood of error

3. Limitations on the number of incorrect logins in a fixed time frame improves security of a traditional password system.  
4. Smudge Attack: On phone that touched the face it was easiest to find password information.  
5. Typing in a numeric code on a keypad is not a type of gesture based authentication.  
6. Following are type of gesture based authentication:

* Connecting dots on a grid
* Drawing a signature on a touch screen
* Swiping multiple fingers in a line or shape

7. Following are method for obtaining a second factor authentication code:

* From an app designed to create codes
* In a text message
* Off a device that generates codes

8. Following are type of biometric authentication:

* Facial recognition
* Free gesture
* Voice analysis

9. Two factor authentication DOES NOT improve the security and usability of a system.  
10. Most secure passwords are collection of words like: **I am not Easy T0 Find**   
instead of likes:

* dz&w4%lfc
* hello etc.

### Usable Security - Usable Privacy

1. Guidelines for usable privacy:

* Make privacy systems match users' expectations from previous experiences.
* Clearly indicate what information will be shared, with whom, and how.
* Make privacy part of the natural workflow

2. A mobile app uses a phone's microphone to listen in the background for commercials, songs, and TV shows that a person is hearing in order to target ads at the user. The app does not store any information about users' conversations nor does it store recordings. Should the app disclose that it is listening to this background sound?

* Yes, users should be informed that sound from their environment is being collected.

3. Alternatives to privacy policies can be as effective in teaching users about how their data is shared.  
4. Following attributes can be automatically inferred on social media, even if users don't provide any obvious clues:

* Intelligence
* Personality
* Sexual Orientation

5. Informed Consent: A person knows how their data is used and competently agrees to that use.  
  
  
6. A website provides an extensive 50-printed-page privacy policy written in common language that describes every detail of how users' data is collected, used, and shared. What is violated here?

* The policy does not meet the requirement of minimal distraction

7.Providing complete and detailed explanations of how data is collected and used can overwhelm the user and lead to a less usable privacy system.