

Security and Usability: Overview

Dr. Neminath Hubballi

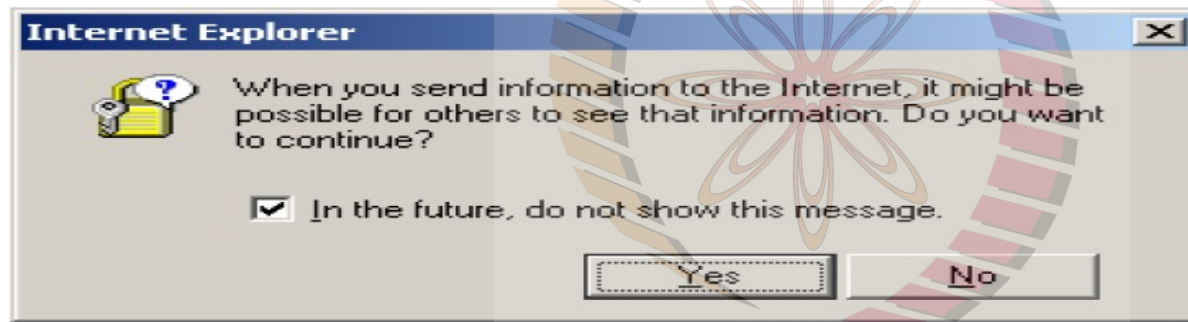
NPTEL

Overview

- ☐ Understanding usability
- ☐ Security v/s usability
- ☐ Usability of authentication systems
 - ☐ Password based authentication
 - ☐ Biometrics based authentication

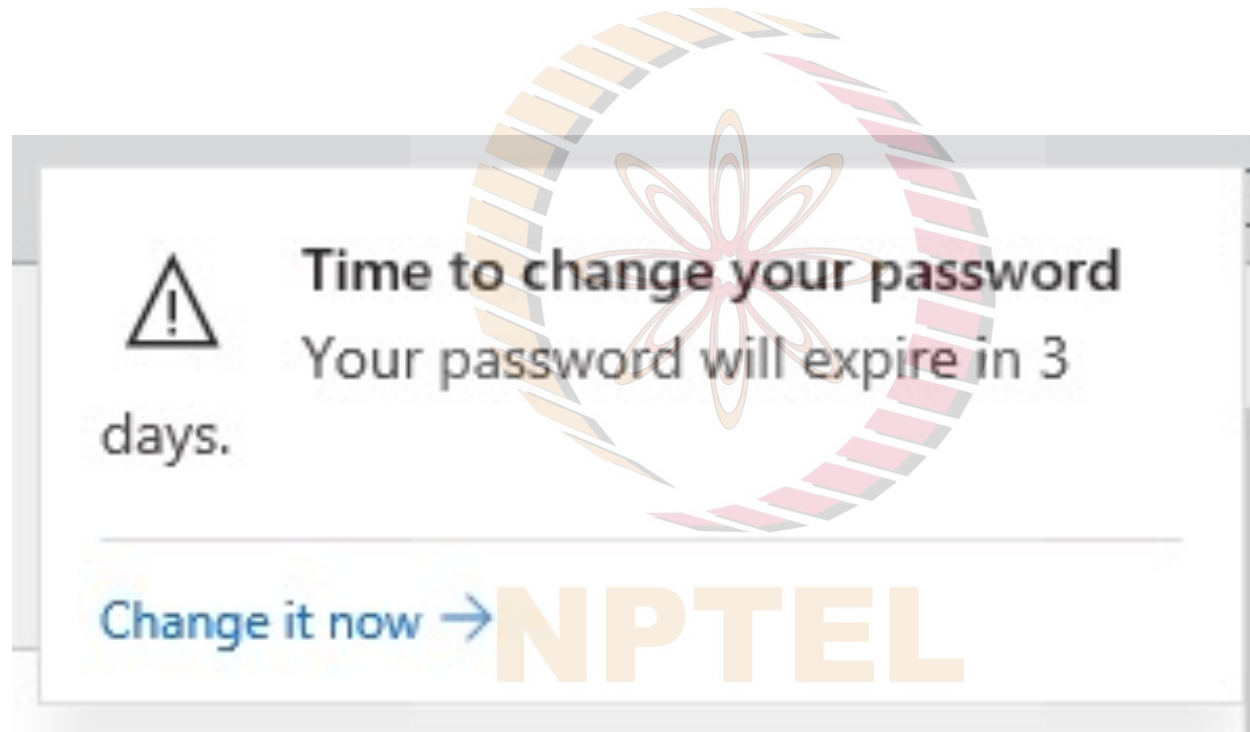


Developers v/s Users



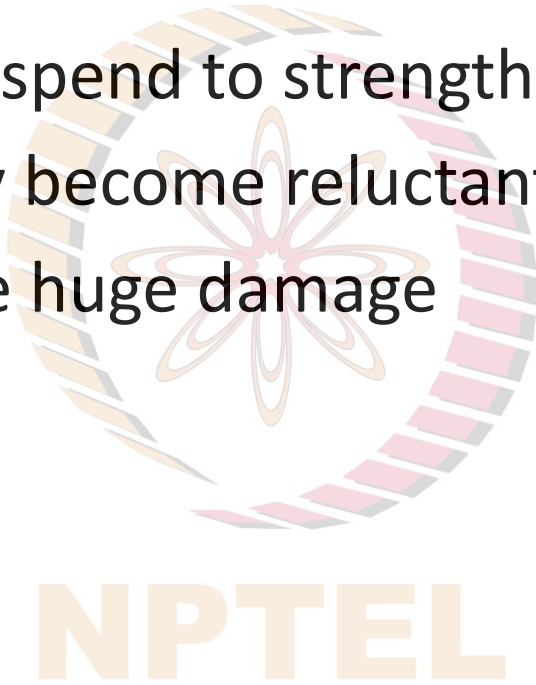
NPTTEL

Password Change Alert



Cyber Attack Consequences

- ☐ Economic fall – Need to spend to strengthen the IT security
- ☐ Avoidance – People may become reluctant to use
- ☐ Catastrophe – Can cause huge damage



Usability

- ❑ General perception: How well the user interface is designed ?
- ❑ It is much more than that !
- ❑ ISO defines it as “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use”
- ❑ Nielsen and Shneiderman define usability with attributes
 - ❑ Learnability
 - ❑ Efficiency of use
 - ❑ Memorability
 - ❑ No catastrophic errors
 - ❑ Subjective satisfaction

Functionality v/s Security

- ❑ Functionality: An application exhibits functionality if design or development goals are met
 - ❑ To whom it interests ?
 - ❑ Nobody wants to spend time fixing something!
 - ❑ Marketing people
 - ❑ Decision makers
- ❑ Security: An application exhibits security if things that should not happen does not happen
 - ❑ Security experts

Security Theory v/s Practice

- ❑ More and more computer attacks are exploiting human weakness

- ❑ Users are not experts of security

- ❑ Having the best does not guarantee you Safety

- ❑ Security solutions like PKI, access control systems are not helping completely



Courtesy Google images, Microsoft (Clip Art)

Why it is Challenging?

- ☐ Security remain challenge for individuals and enterprises to
 - ☐ Understand
 - ☐ Manage and
 - ☐ Configure
- ☐ Earlier – security was network administrator's problem
- ☐ Security feature can be an obstacle for the work
 - ☐ Disabled or bypassed
- ☐ Security often becomes obstacle for functionality
 - ☐ Ignore security !

What is the Takeaway ?

- ❑ Human (User) is in the loop
 - ❑ She participate in security critical functions
- ❑ Examples
 - ❑ Settings in browsers
 - ❑ Choosing passwords
 - ❑ Running unauthorized software
 - ❑ Antivirus software on detecting a malicious file asking the user to
 - ❑ Quarantine
 - ❑ Delete
 - ❑ Continue
- ❑ Problem is they do not do it correctly because
 - ❑ Either they do not know how to do it
 - ❑ It is difficult to do it
- ❑ The takeaway is “do not involve end user in security critical functions (decisions) or make it very obvious as to what to do”
 - ❑ Strong cryptography, Provably correct protocols and Bug-free code will not provide security

Where Users Go Wrong ?

- ☐ Fail to click on encryption button
- ☐ Mis-configure their systems
- ☐ Choose weak cryptographic keys
- ☐ Do not secure the cryptographic keys



How Security and Usability Relate ?

- ❑ They both trade off
 - ❑ Ex: Periodic password change may be good for security but if a user has to remember a complex password.
- ❑ Standard practices are available for UI usability testing but specification and design stage models are not there
- ❑ Throughout development life cycle
 - ❑ Security, privacy and usability should be addressed

Fundamental Questions

- ☐ Does added security make things more difficult to use?
- ☐ Will people always resent the extra steps?



User Authentication

- ☐ Usually done through
 - ☐ Something user knows
 - ☐ Something user has
- ☐ What are the dangers
 - ☐ Stolen
 - ☐ Forgotten
 - ☐ Disclosed
 - ☐ Lost



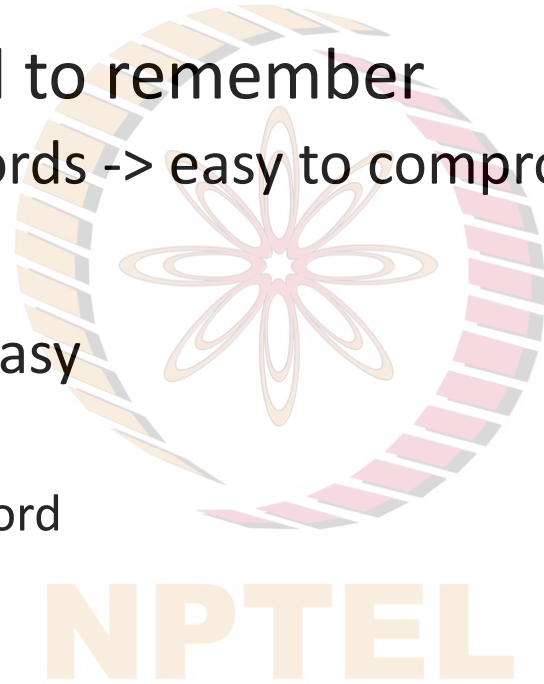
Password Usability

- ☐ Password complexity
- ☐ Restrictions
- ☐ Breaking
- ☐ Multiplicity of passwords, accounts



Graphical Password

- ☐ Text passwords are hard to remember
 - ☐ Users select easy passwords -> easy to compromise
- ☐ Graphical passwords
 - ☐ Recollecting pictures is easy
 - ☐ Are of two types
 - ☐ Recognition based password
 - ☐ Recall based password



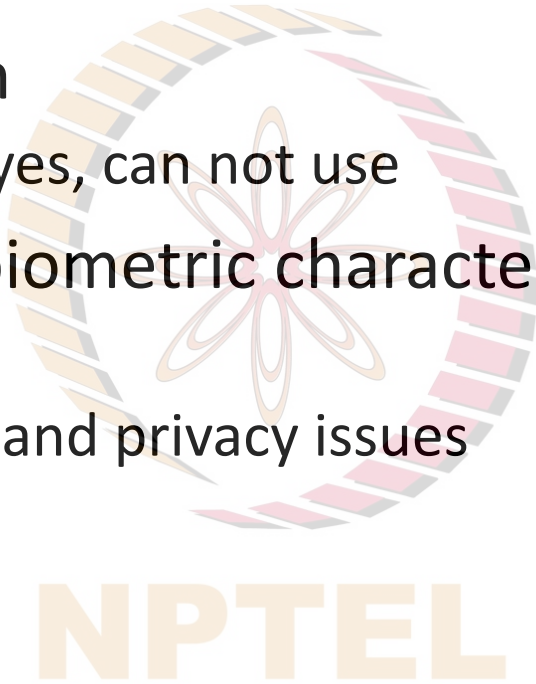
Biometrics-User Authentication

- ☐ Biometrics based authentication is more robust
- ☐ Measurable
 - ☐ Fingerprint
 - ☐ Iris
 - ☐ Voice data



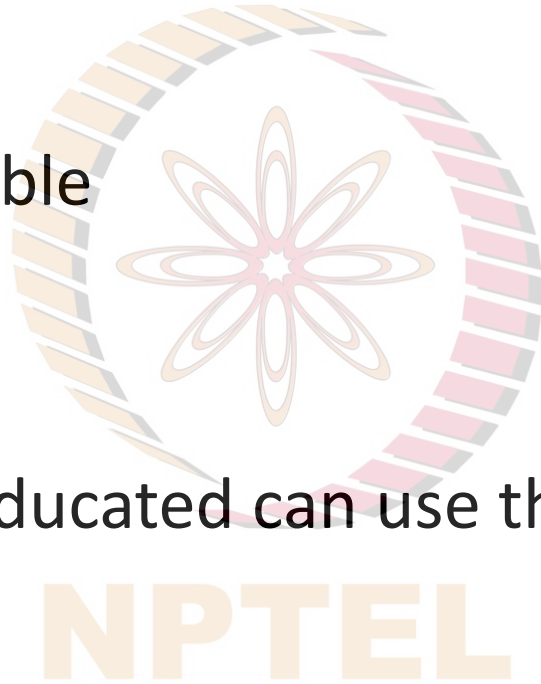
Biometric-Usability Aspects

- ☐ User biometric collection
 - ☐ People without fingers, eyes, can not use
- ☐ Creating and Storing of biometric characteristics
 - ☐ Multiple samples
 - ☐ Where to store - Security and privacy issues
 - ☐ Card
 - ☐ Database
- ☐ Verification
 - ☐ Incorrect scanning
 - ☐ Decision making - threshold



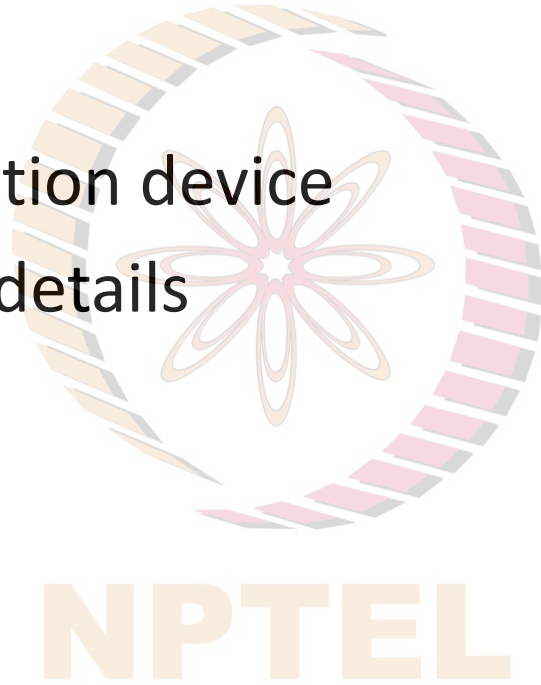
Biometric- Advantages

- ☐ Authenticate the user
- ☐ Unique and not changeable
- ☐ Difficult to copy
- ☐ Not a secret
- ☐ Even a user who is not educated can use the system



Biometric-Disadvantage

- ☐ Person with disability
- ☐ Trust on biometric collection device
- ☐ Privacy concerns - DNA details



Other Authentication Methods

- ☐ PIN

- ☐ Two-factor authentication



A system focused on usability

- ☐ A compromised machine is not usable
- ☐ Reliability or availability might suffer
- ☐ Will users notice?



Developers v/s Users

- ❑ “Defend but Do not Ask” - Building something that relies on user education to be effective is a recipe for disaster
- ❑ Best thing is to design the system such that it does not need to ask the user
 - ❑ Invariably she clicks on “OK” or whatever else to continue doing her job
- ❑ Do the right thing but do not show it to user
 - ❑ The best UI in a security warning is the one that is not there

Developers v/s Users

- ❑ Make the default settings secure
- ❑ Use automation when possible
- ❑ Don't "punt" to the user when there's a problem
- ❑ *Path of least resistance*

