

# User Interface vs. Security

Tom Vogt <[tom@lemuria.org](mailto:tom@lemuria.org)>

# UI vs. Security

What's the weakest link in security ?



# UI vs. Security

## The dumb user

- clicks on anything
- chooses weak passwords
- installs insecure software
- falls for phishing, etc.
- uses IE, Outlook, etc.



# UI vs. Security

**Wrong!**

- The user isn't the problem
- He'll do whatever seems best in context (NLP!)
- We control the context
- We don't control the user



# User Interface Design for Security

# User Interface Design for Security

# The Trouble with Passwords

Messaging Server Version 6.1 Configuration Wizard.

**Sun**  
microsystems

**Password for all admin accounts**

Enter a password of at least 16 characters. Use special characters and numbers. Do not use names or words from a dictionary. Do not use dates, sizes, room numbers or other meaningful numbers.

Make your password difficult to guess, but choose something you can remember. Choose a password you can type quickly, without looking at the keyboard.

Never write your password down.

Do not choose a password you are using for something else already.

Password

Enter password:

Re-enter password to verify:

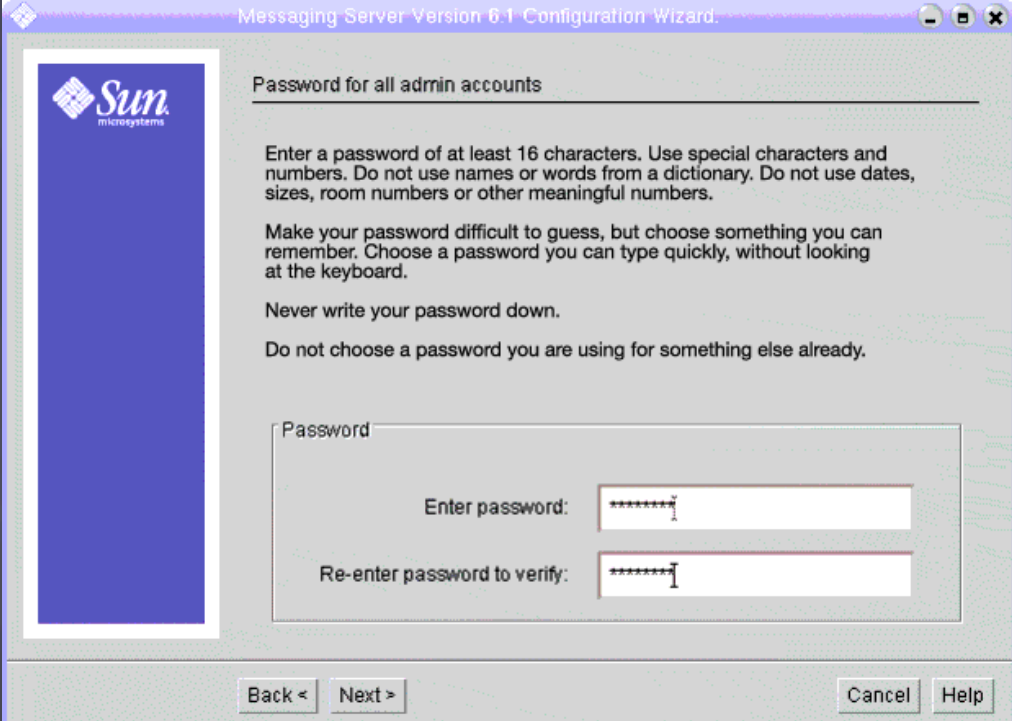
Back < Next > Cancel Help



# Passwords

Users choose weak passwords because passwords are a weak system

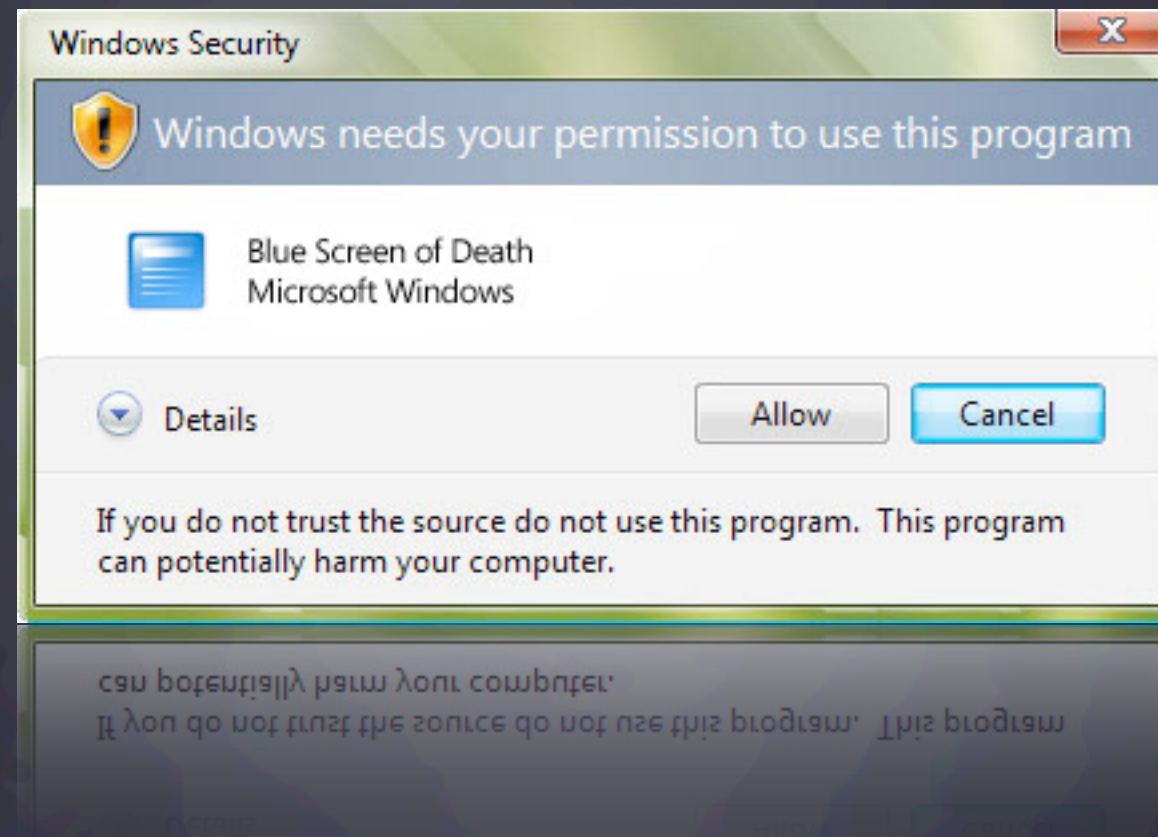
- Conflict of human memory and machine requirements
- Enforcing requirements weakens security
- Inhuman requirements lead to (unconscious) sabotage



The screenshot shows a Windows-style dialog box titled "Messaging Server Version 6.1 Configuration Wizard". On the left is a blue vertical bar with the Sun Microsystems logo. The main area has a title "Password for all admin accounts" and instructions: "Enter a password of at least 16 characters. Use special characters and numbers. Do not use names or words from a dictionary. Do not use dates, sizes, room numbers or other meaningful numbers." It also says: "Make your password difficult to guess, but choose something you can remember. Choose a password you can type quickly, without looking at the keyboard." and "Never write your password down. Do not choose a password you are using for something else already." Below the text are two input fields: "Enter password:" and "Re-enter password to verify:", both containing masked text (asterisks). At the bottom are buttons for "Back <", "Next >", "Cancel", and "Help".



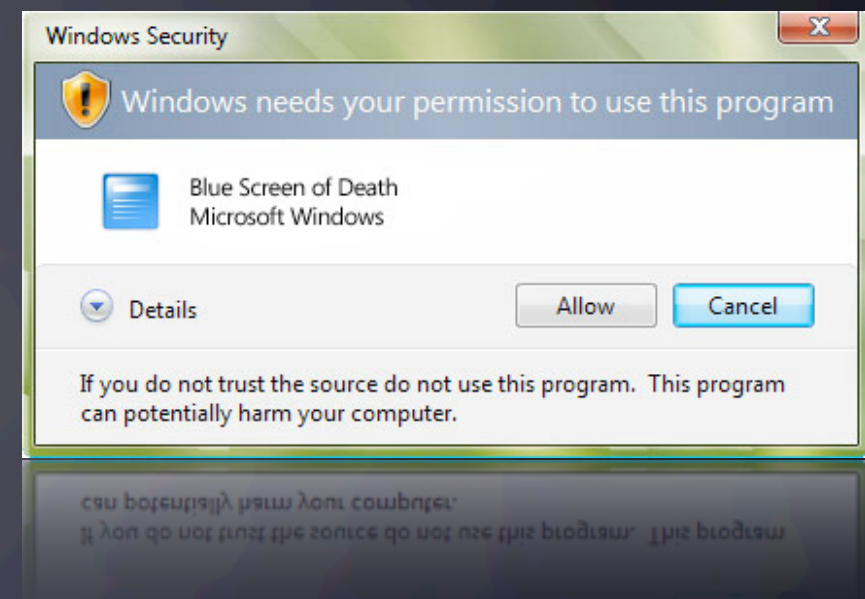
# The Trouble with Confirmation Dialogs



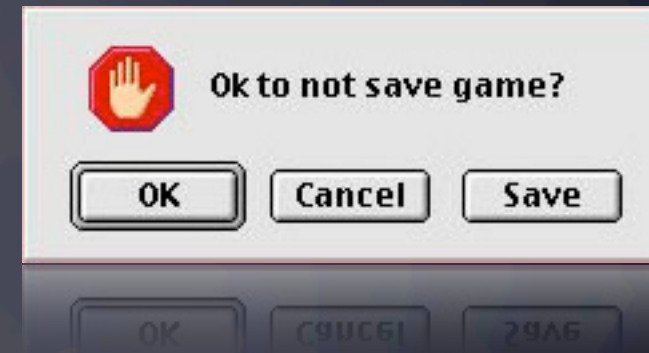
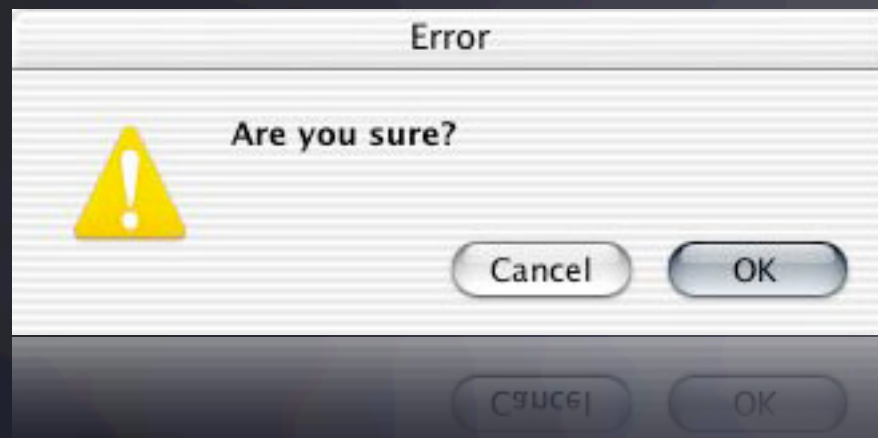
# Confirmation Dialogs

Confirmation dialogs are the wrong answer.

- Interrupt workflow
- Condition the wrong response if used in excess
- Shift responsibility
- are often confusing



# More Bad Examples



# The Trouble with Phishing and Trojans

**From:** admin@reply8647.user.ebaybid.com  
**Date:** Wednesday, October 11, 2006 7:50 AM  
**To:** @hotmail.com  
**Subject:** RE: Alert Message 99820565515184

1. Questionable Sender's Address

eBay sent this message to you. If you are not a member, please delete this message. If you are a member, please click the link below to verify your account. Your registered name is [redacted] (member).  
Learn more.

2. Sense of Urgency

**Hurry! Message for @hotmail.com. Update Now!**

Dear @hotmail.com,

We are contacting you to remind you that on 10 OCT 2006 we identified some unusual activity in your account coming from a foreign IP address: 201.8.43.167 ( IP address located in China ). We have been notified that a card associated with your account has been reported as lost or stolen and involved in fraudulent transactions, or that there were additional problems with your card.

3. Non-US Dating Format

According to our site policy you will have to confirm that you are the real owner of the eBay account by completing the following form or else your account will be marked as fraudulent , and will remain open for investigation. You will pay for the fees wich will result from the financial transactions between eBay and FIT ( Fraud Investigations Team ).

4. Threat!

[https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&co\\_partnerId=2&pUserId=&siteId=0&pageType=&pa1=&i1=&bshowgif=&UsingSSL=yes](https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&co_partnerId=2&pUserId=&siteId=0&pageType=&pa1=&i1=&bshowgif=&UsingSSL=yes)

eBay's Privacy Policy and Law Enforcement Disclosure: We care deeply about the privacy of the eBay community and will protect the privacy of our members even while working closely with law enforcement to prevent criminal activity. If you have any questions, please visit eBay's Privacy Central for more information.

5. Link & URL in Status Bar Doesn't Match

<http://user47id.com/.../>

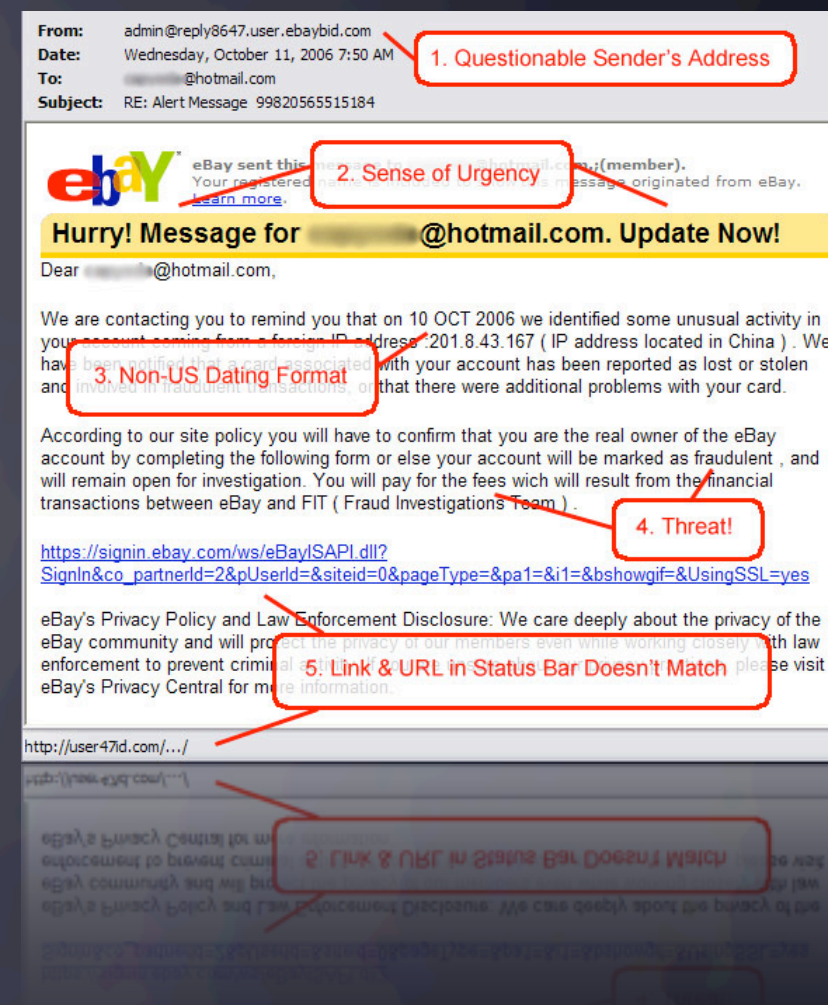
6. Link & URL in Status Bar Doesn't Match



# Phishing and Trojans

Phishing works because the user interface sucks

- Human perception works the exact opposite
  - bigger == more important
  - colours == important
  - center == important
- Info needed to spot a phishing attack often hidden in status/URL bar - if visible at all!



# Phishing and Trojans

## Good News

- recognized as a problem
- countermeasures are being tested and deployed
- many solutions target the proper level: The UI

## Bad News

- most solutions still in experimental stage
- many available solutions too specific (ebay/paypal toolbar)
- phishing is big business not likely to just pack up and go away

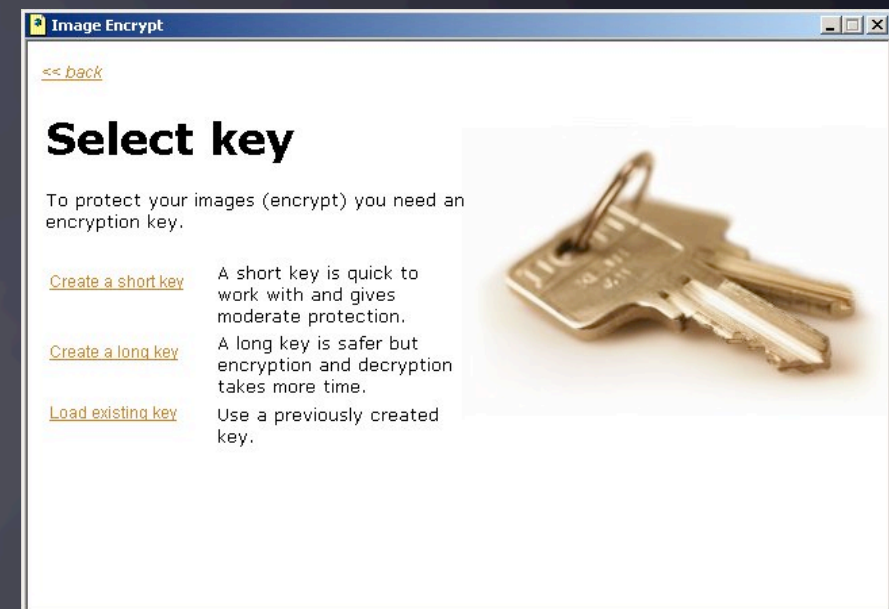


# The Trouble with Metaphors



# Metaphors

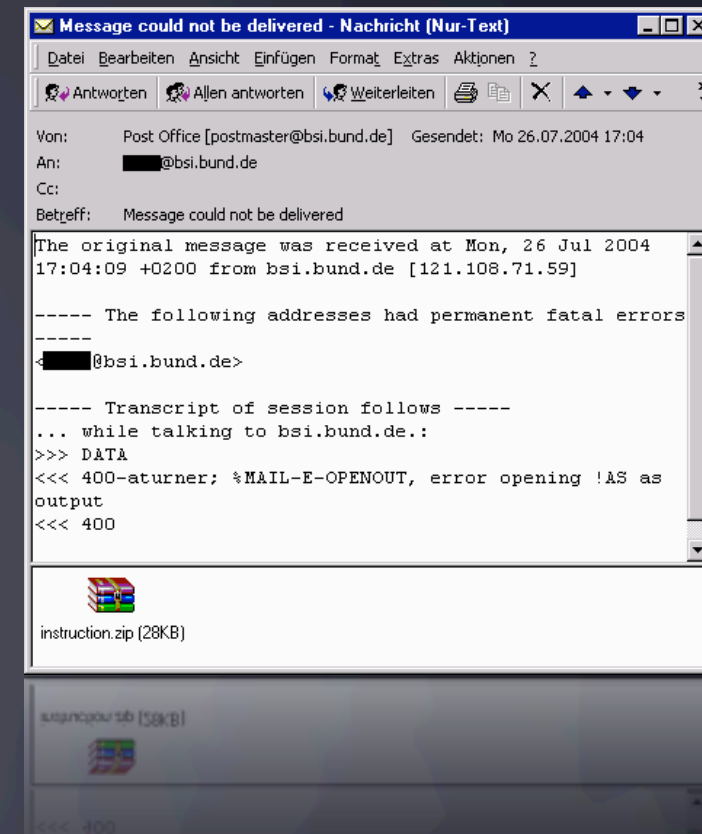
- very useful shortcuts to understanding
- but often used carelessly
- transporting wrong or unintended meaning



# Metaphors

one especially bad example:

- taken too far, we see applications as documents
- ... opened with - themselves
- blurring the line between data and code:

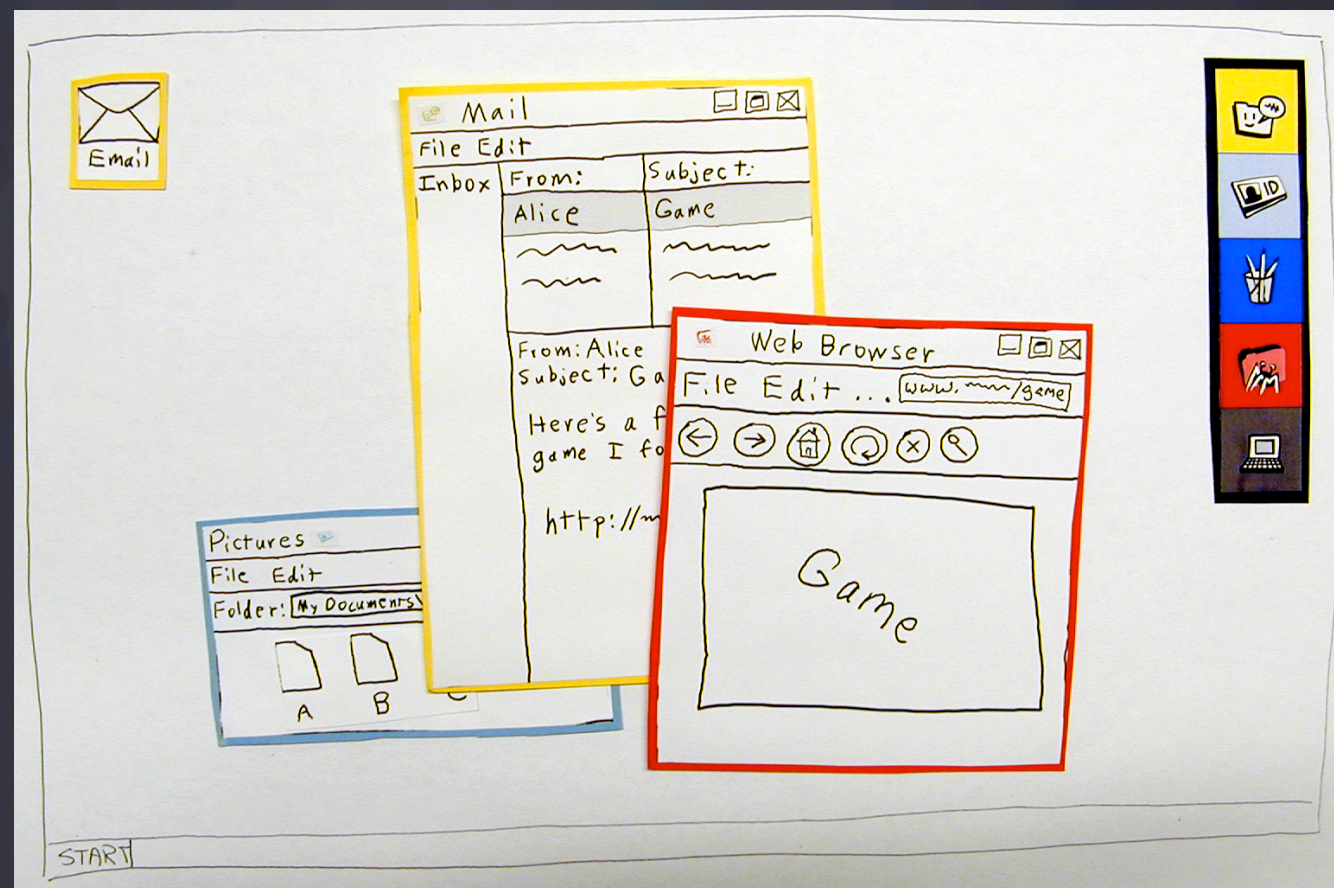


“document”	data	code
information for me	information for me	instructions for machine
safe to handle (except for papercuts)	safe to handle (except for overflows)	unsafe at any speed



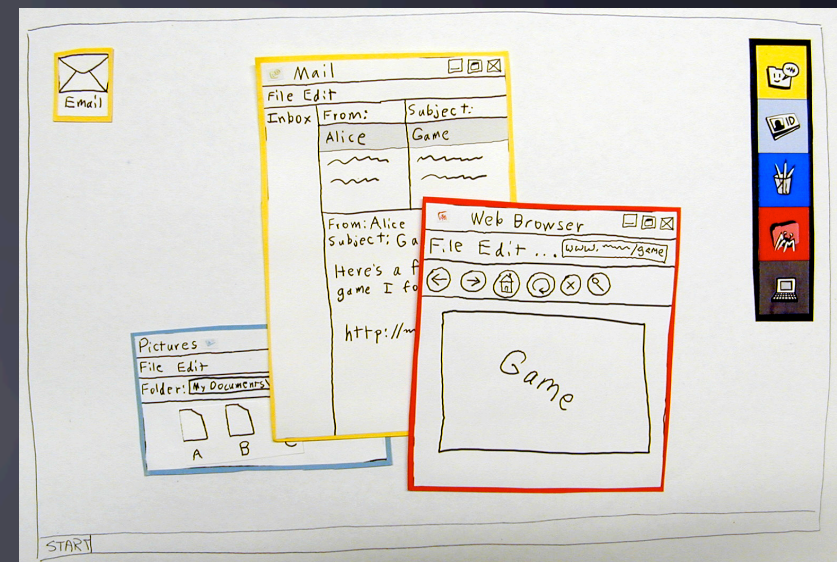
# example of doing it right:

# Chameleon



# Chameleon

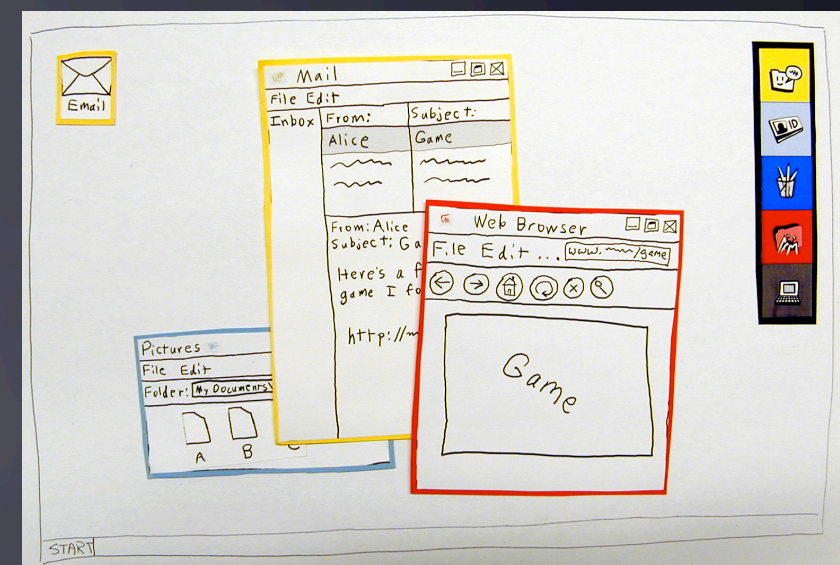
- role-based execution environments for apps
- similar to sandboxing
- visible indication of each windows role
- coarse roles sufficient:
  - system
  - vault
  - default
  - testing





# Chameleon

- good metaphor: Trust
  - people understand not to trust everyone
  - people understand roles - the wife gets the keys, but not the mailman
- feedback loop kept intact
  - visual feedback about trust levels apps operate under





# Conclusion

# UI vs. Security

## The “dumb” user

- clicks on anything
  - ➡ has been taught that’s how you access stuff
- chooses weak passwords
  - ➡ hard passwords are not for humans
- installs insecure software
  - ➡ system allows untrusted apps more than user expects
- falls for phishing, etc.
  - ➡ tests show security experts don’t score much better...
- uses IE, Outlook, etc.
  - ➡ ok, got me on that one, that is a user problem ☺

# Conclusion

- Users are not the problem, the user interface is.
- Good user interface design:
  - put responsibility where it belongs
  - be unobtrusive
  - speak the language of the recipient
  - do not expect non-human behaviour from humans

# UI and Security

- Considering human factors will improve security
  - higher acceptance
  - less errors
- Respecting user and his needs will gain cooperation
  - people like to be treated with respect

# Principles

I. user profiling:  
know your user, speak  
his language

II. metaphor:  
borrow behaviours  
from contexts familiar  
to users

III. exposure:  
let the user clearly see  
his options

IV. coherence:  
behaviour should be  
consistent

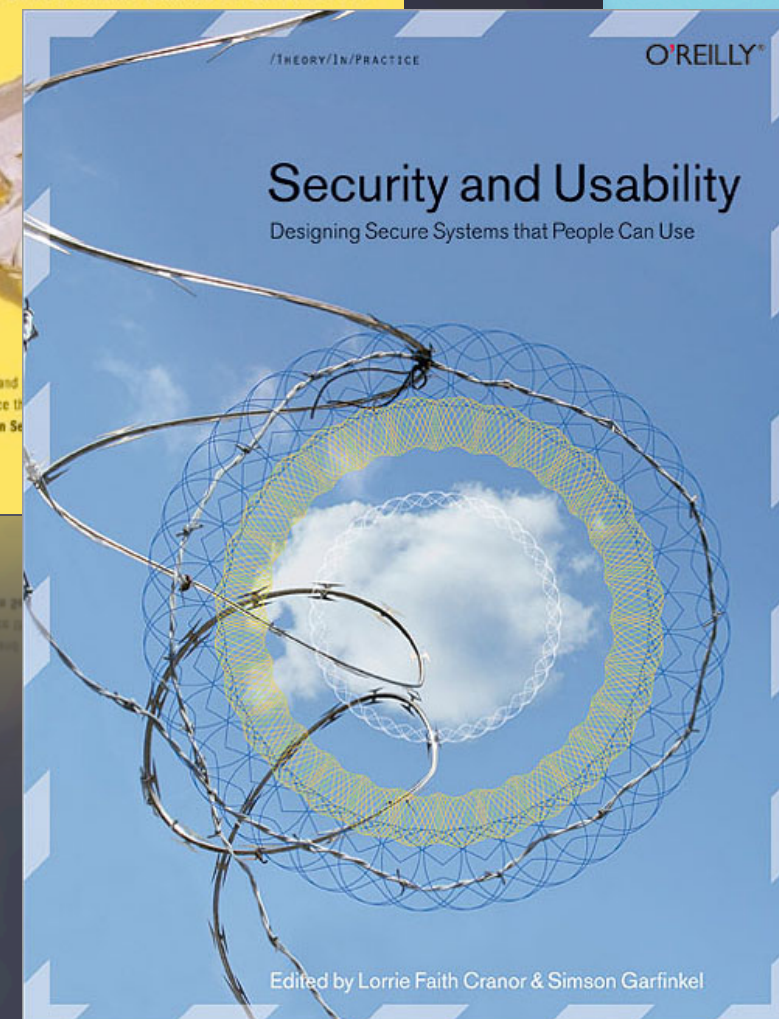
V. context and workflow:  
adapt to the modus the  
user is currently in

VI. user testing:  
recruit help to spot  
inevitable defects



# Some References

- Security and Usability  
ISBN 0596008279
- The Paradox of Choice  
ISBN 0060005696
- Language, Thought and Reality  
ISBN 0262730065



## Language Thought and Reality

Selected Writings of  
Benjamin Lee Whorf

edited by John B. Carroll