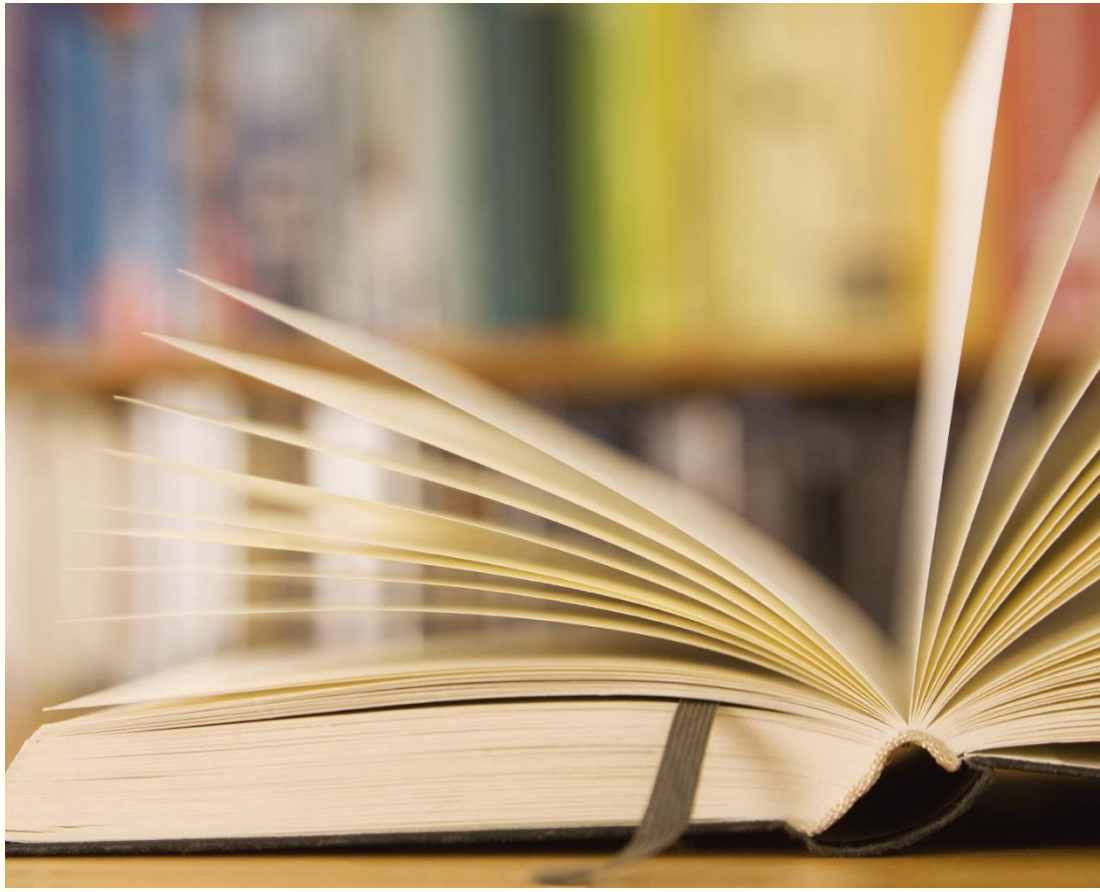
USABILITY AND PSYCHOLOGY

(CHAPTER 2, "SECURITY ENGINEERING" BY ROSS ANDERSON)



Security Seminar April 5, 2016

Lecturer: Prof. Orr Dunkelman Presenter: Yuri Emelianov

Agenda

- Introduction & Motivation
- Attacks based on Psychology
  - Pretexting
  - Phishing
- Phishing Countermeasures & Future
- Insights from Psychology Research
  - Brain VS Computer (cons/pros)
  - Social Psychology
- Passwords
- Summary

Introduction & Motivation

"Only amateurs attack machines; professionals target people"

B.Schneier

- Real attacks exploit psychology at least as much as technology
- Online crime based on psychology attacks could be divided to:
  1. *Phishing*
  2. *Pretexting*
- *Social engineering*: psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.

Attacks Based on Psychology:
Pretexting

Is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. An elaborate lie, it most often involves some prior research or setup and the use of this information for impersonation (*e.g.*, date of birth, Social Security number) to establish legitimacy in the mind of the target. (from https://en.**wikipedia**.org)

Attacks Based on Psychology:
Pretexting(continue)

Used to fool a business into disclosing customer information as well as by private investigators to obtain telephone records, banking records and other information directly from company service representatives. The information can then be used to establish even greater legitimacy under tougher questioning with a manager, *e.g.*, to make account changes, get specific balances.

Attacks Based on Psychology:
Pretexting(continue)

Used to impersonate co-workers, bank (any other individual) who could have perceived authority or right-to-know in the mind of the targeted victim. The pretexter must simply prepare answers to questions that might be asked by the victim. In some cases, all that is needed is a voice that sounds authoritative, an earnest tone, and an ability to think on one's feet to create a pretextual scenario.

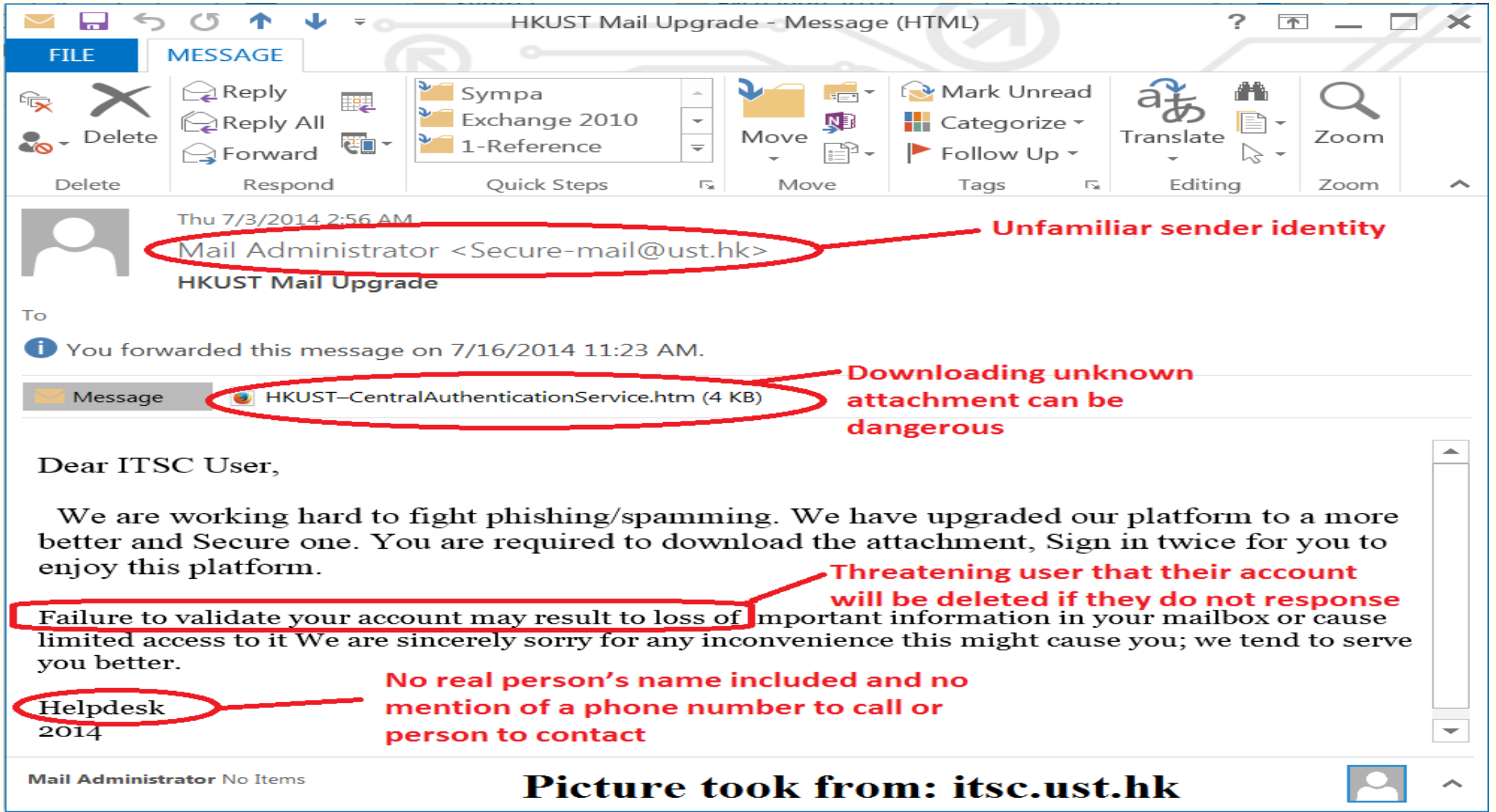
Attacks Based on Psychology:
Pretexting(continue)

- How to prevent?
- Approaches:
  1. Trainings
  2. Special attacks on own staff

Attacks Based on Psychology:
Phishing

Is a technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business—a bank, or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN. (from https://en.**wikipedia**.org)

Attacks Based on Psychology:
Phishing - Example



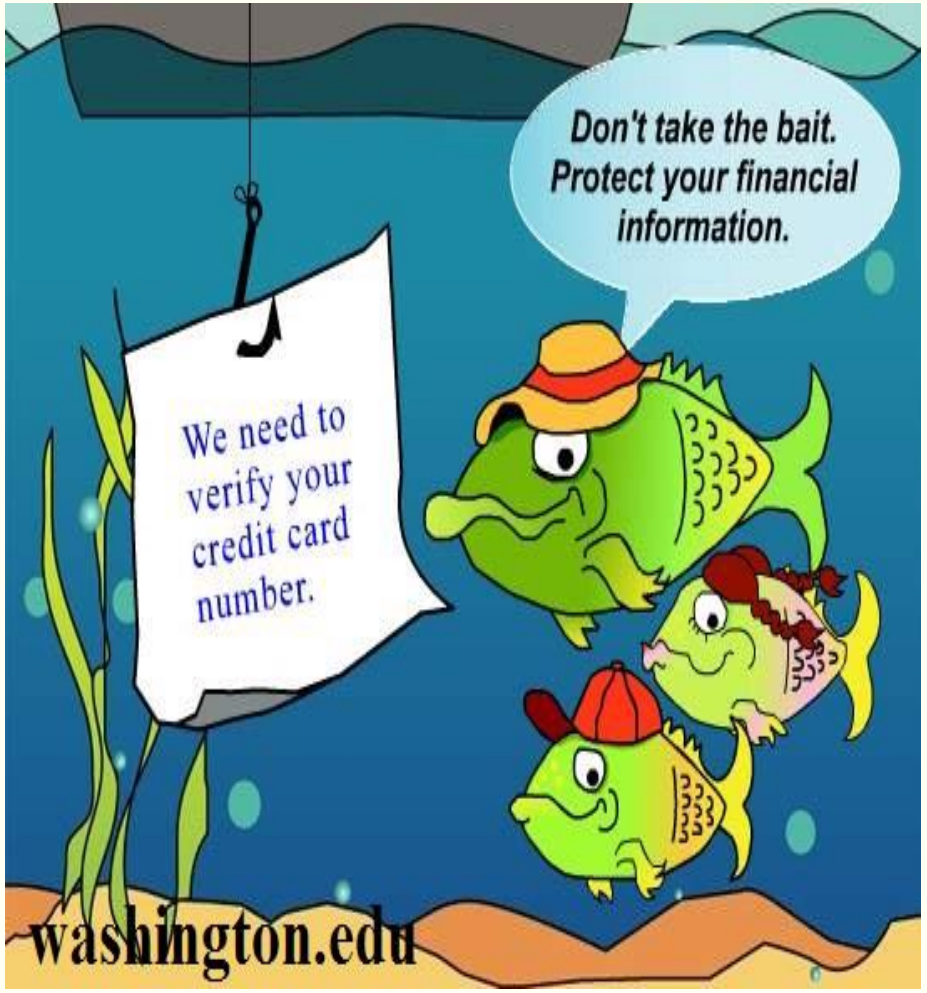
Attacks Based on Psychology : Phishing(continue)

- Phishing business has plenty room for growth
- In many ways harder problem for a company to deal with than pretexting, since the targets are not your staff but your customers

For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless a link provided was clicked to update a credit card.

Attacks Based on Psychology:
Phishing(continue)

Because it is relatively simple to make a Web site resemble a legitimate organization's site by mimicking the HTML code, the scam counted on people being tricked into thinking they were being contacted by eBay and subsequently, were going to eBay's site to update their account information.



Phishing Countermeasures

- Password Manglers
- Using the Browser's Password Database
- Soft Keyboards
- Customer Education
- Microsoft Passport
- Phishing Alert Toolbars
- Two-Factor Authentication
- Trusted Computing

Phishing Countermeasures:
Future

- Phishing trade grow substantially
- Will get smarter and harder to tell from real emails
- Will forge emails from your mother
- More attempts to interfere in the identity market (biometrics)
- Invest most of security budget in the back end

Insights from Psychology Research:
What the Brain Does Worse Than the Computer

We still do not understand one central problem – the nature of consciousness.

- Slips and lapses at the level of skill: inattention can cause a practiced action to be performed instead of an intended one.
- Mistakes at the level of rules: people are open to errors when they follow wrong rule.
- Mistakes at the cognitive level: people don't understand problem. Example

Insights from Psychology Research:
Perceptual Bias and Behavioral Economics

The most promising field of psychology for security folks

- Kahneman & Tversky → prospect theory

Main aspects:

- most of us not just more afraid of losing something we have, than of **not making a gain** of equivalent value

- People just plump for the standard configuration of a system, as they assume it will be **good enough**

Insights from Psychology Research:
Perceptual Bias and Behavioral Economics(continue)

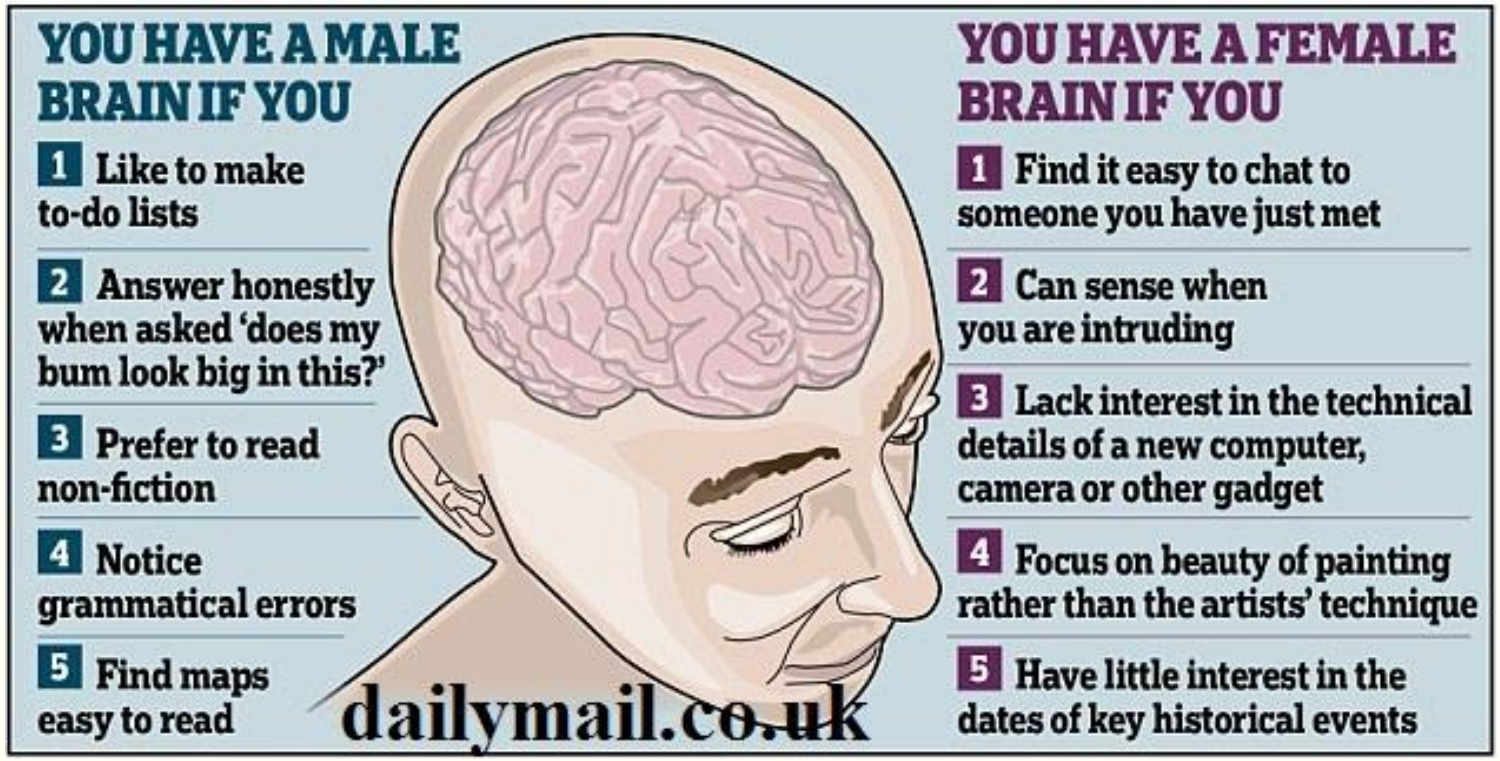
- Many frauds work by appealing to our atavistic instincts to trust people more in certain situations or over certain types of decisions
- Biases: We are less afraid when we're in control, more afraid of risks to which we've been sensitized, more afraid of uncertainty

Insights from Psychology Research:
Different Aspects of Mental Processing

- Mind as rational & emotional components – ‘affective’ & ‘cognitive’ systems
- Fundamental attribution error
- Affect heuristic
- Cognitive overload
- Social contexts

Insights from Psychology Research:
Differences Between People

- Male VS Female
- Human brains: type S (systematizer) VS type E (empathizers)



Insights from Psychology Research:
Social Psychology

Explains how the thoughts, feelings & behavior of individuals are influenced by the actual, imagined, or implied presence of others.

- Three particularly famous experiments and outcomes:

1. Authority rather than their conscience
2. People could be induced to deny the evidence of their own eyes in order to conform to a group
3. Normal people can behave wickedly even in the absence of orders

Insights from Psychology Research:
Social Psychology(continue)

Cognitive dissonance theory

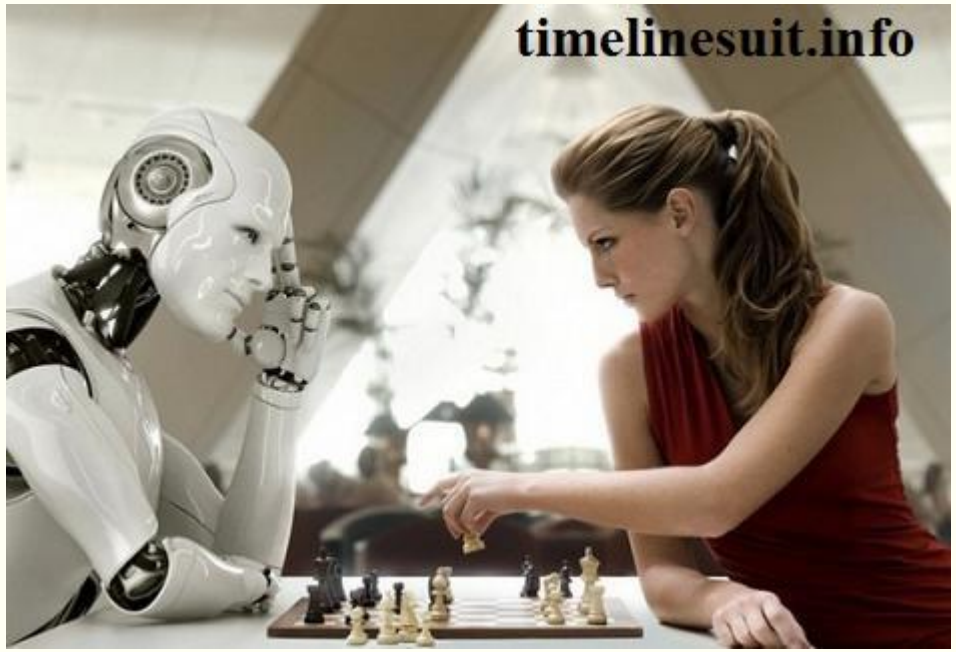
Main aspects:

- Rejection information that conflicts with their views or might undermine their self-esteem

- People are remarkably able to persist in wrong courses of action in the face of mounting evidence that things have gone wrong

Insights from Psychology Research:
What the Brain Does Better Than the Computer

- Recognizing other human visually
- Image recognition generally
- Understanding speech, particularly in noisy environments, and at identifying speakers



Passwords

- Biggest practical problem facing security engineer today
- The same passwords used over & over again
- Managing passwords is a serious problem that mixes issues of psychology with technical issues
- *Human-factors* issue: too long or complex, might have difficulty entering it correctly. *Example:* South Africa prepaid electricity meters
- *Activation codes* software: error rate increases. *Example:* U.S. firing codes

Passwords:
Difficulties with Reliable Password Entry

- Three options of authenticating users to systems:
  1. What you have [remote car door key]
  2. What you know [password] ← most common option
  3. What you are [fingerprint or iris pattern]

Passwords:
Difficulties with Remembering the Password

- *Human-factors* issue: people often find them hard to remember

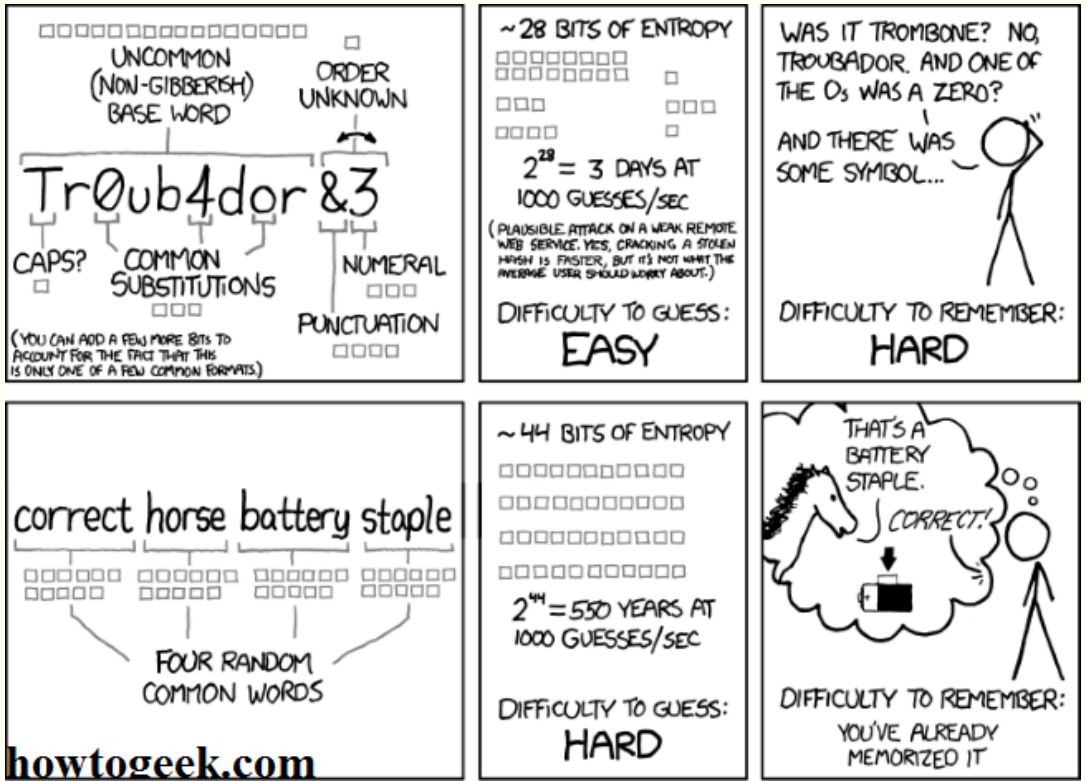
  "Choose a password you can't remember & don't write it down"

Problem related to password memorability:

- native password choice
- user abilities and training
- design errors
- operational failures

Passwords:
Difficulties with Remembering the Password: Native Password Choice

- People have studied what sort of passwords are chosen by users who are left to their own devices
- Up to 25% of passwords could be guessed depending on the amount of effort
- Users change password rapidly to exhaust the history list & get back to favorite



Passwords:
User abilities & Training, Design Errors, Social-Eng. attacks

- Experiment of choosing good password
- Making passwords memorable are frequent source of design errors
- Unskilled people
- “PIN” discussions
- Bad practices by banks, bad customer training
- Trusted Path

Summary

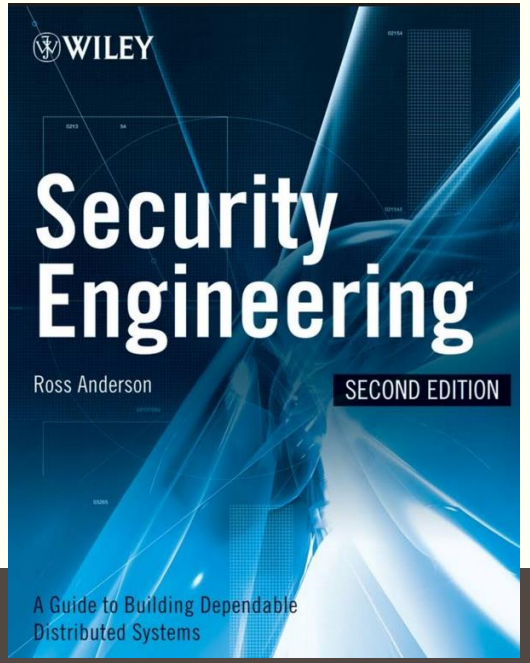
There is no “magic bullet” in sight

- Usability is one the most important and yet hardest design problems
- Most real attacks nowadays target the user
- As technical protection improves, bad guys will target the users
- Phishing is the most rapidly growing threat to online banking systems
- Harden your system enough for the bad guys to hit your competitor

BIBLIOGRAPHY:

Ross, Anderson. Security engineering : a guide to building dependable distributed systems

http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c02.pdf

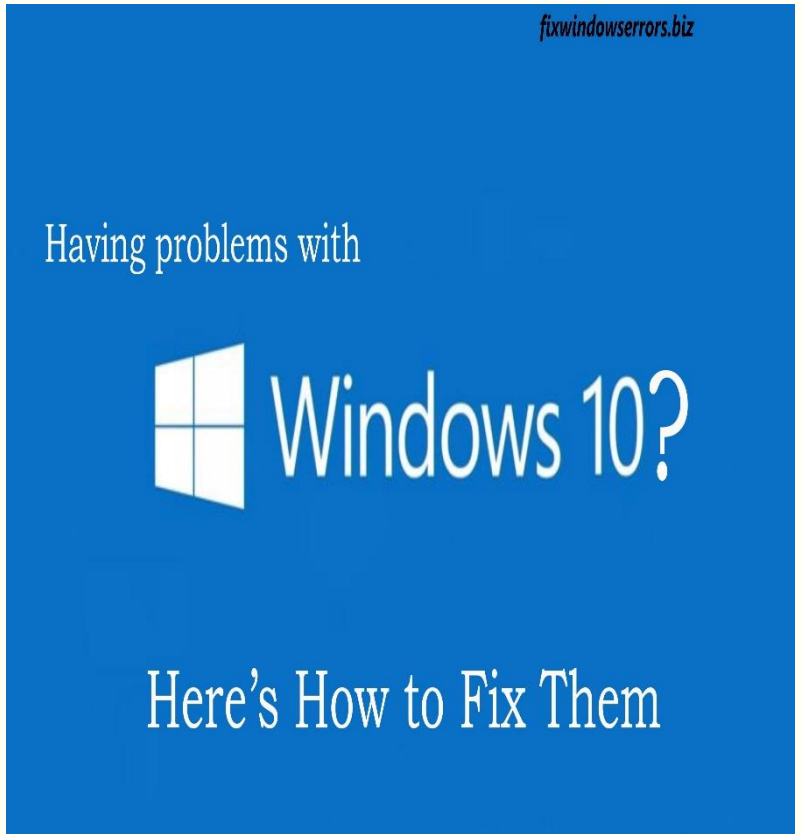


Thank you for your attention!

Backup

System Issues

- Restrict the number of password guesses
- Target attack on one account
- Attack to penetrate any account on a system
- Attack to penetrate any account on any system
- Service denial attack



System Issues (continue)

- Can you deny service?
- Protecting Oneself or Others?

System Issues:
Attacks on Password Entry

- Interface design
- Eavesdropping
- Technical Defeats of Passwords Retry Counters
- Attacks on password Storage
- One-Way Encryption
- Password Cracking [dictionary attack]
- Absolute Limits

System Issues: CAPTCHAs

- Completely Automated Public Turing Test to Tell Computers and Humans Apart
- Brain strengths rather than its weakness
- IDEA: Program generates some random text and produces a distorted version of it that the user must decipher
- NOT WORKING