



# Usability Design for Security



Chung, Kyungho Ph.  
D. KISA

# Contents

I

What is wrong?

II

UI of Security

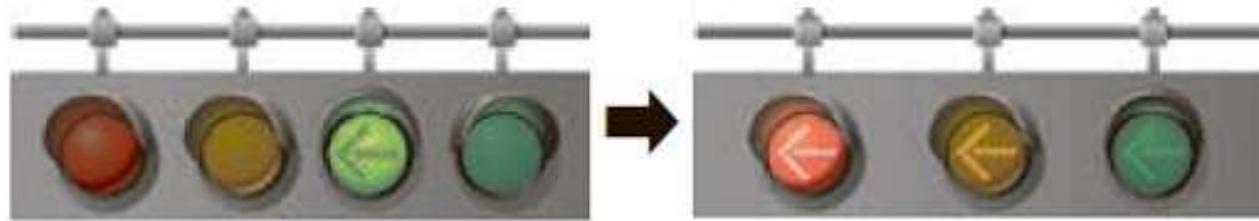
III

HCI Issues

IV

Usability Design

# 1. What is wrong?



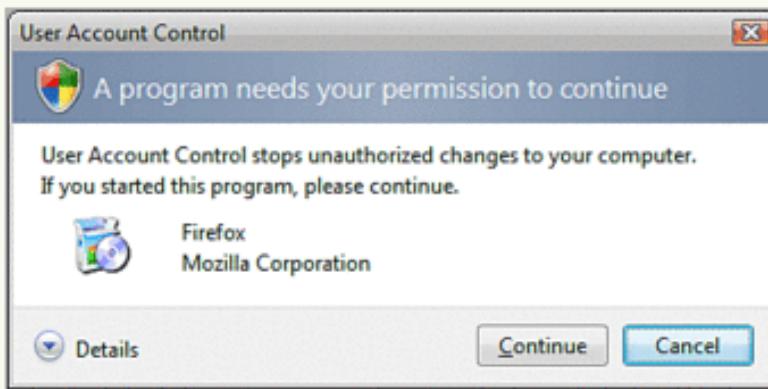
# 1. What is wrong?

## The 10 Biggest Tech Failures of the Last Decade

VISTA

### Windows Vista Tip: Disable annoying "Need your permission to continue" prompts

By Gina Trapani, 8:30 PM on Thu Jan 25 2007, 413,031 views



Windows Vista's User Account Control security "feature" - which I like to call Sir Obnoxious Naggy McNag - is bound to drive any power user batty within an hour of downloading, installing and configuring your favorite programs. If you hate Vista for asking you *every single time you try to do something* if you're sure you want to, then disable User Account Control. The How-To Geek's got the details:



## Full List

### FAILURE TO LAUNCH

Tech Malfunction

Microsoft Vista

Gateway

HD DVD

Vonage

YouTube

Sirius XM

Microsoft Zune

Palm

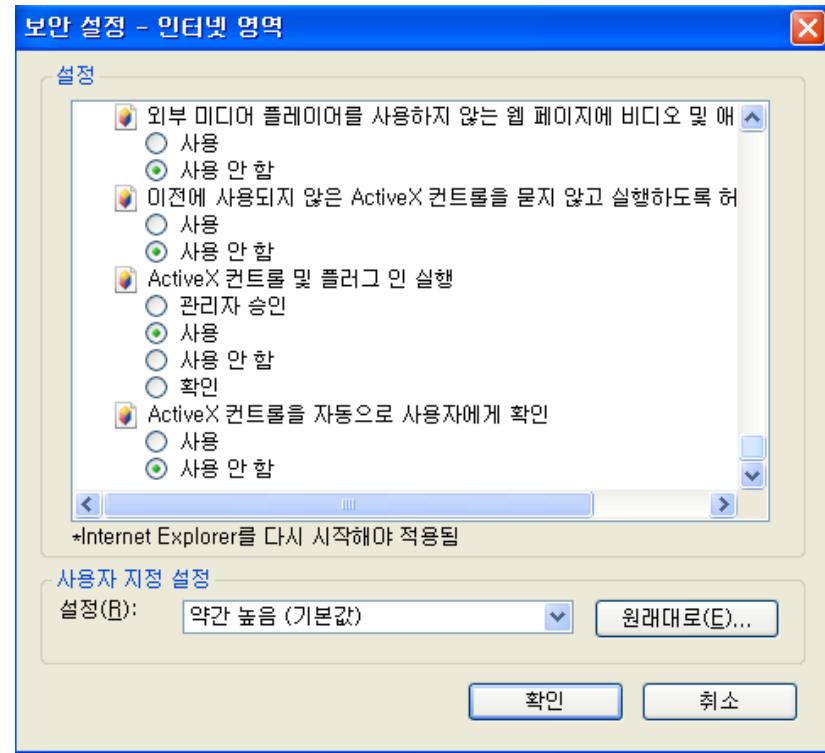
Iridium

## 1. What is wrong?

---

- Lack of understanding for users and tasks
  - Fail to provide users' psychological acceptance
  - Fail to provide usable security
- Users care only their tasks, not security
  - Security is not a task goal
  - Often interfere with usability
- Additional effort, cost to comply
  - Too complex, too difficult

## 2. User Interface of Security



# HCI Issues: Human Psychology

- How secure is enough secure?
  - Fail to provide users' trust in Internet banking

Measures	Type	Threat	HCI Issue	Location
ID/PW	User knows	Dictionary Attack Social Eng.	Memory	User Memory
PKI	User has	Hacking	Theft, Lost	PC/USB
PW for PKI	User knows	Dictionary Attack Social Eng.	Memory	User Memory
Security Card	User has	Hacking ?	Theft, Lost	–
OTP	User has	–	Theft, Lost	–
Secret Number	User knows	Dictionary Attack Social Eng.	Memory	User Memory

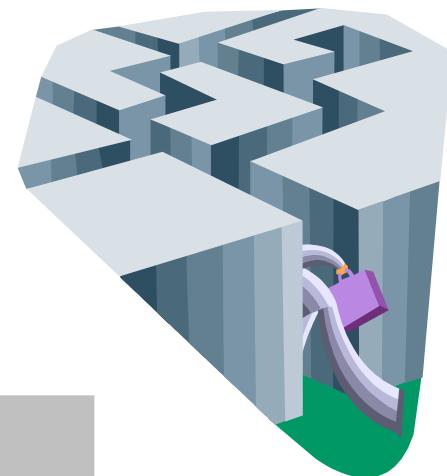
# HCI Issues: ID/PW

- US Federal Information Processing Guidelines
  1. Passwords must be strong, i.e. a pseudo-random mixture of letters, numbers and characters
  2. Users should have a different password for each system
  3. Password should be changed at regular intervals, and accounts of users who do not comply deleted and suspended

Q: I have 30 active ID for e-banking(2), e-trading(1), mail(5), cafe(2), websites (20+). Can I comply with these guidelines?

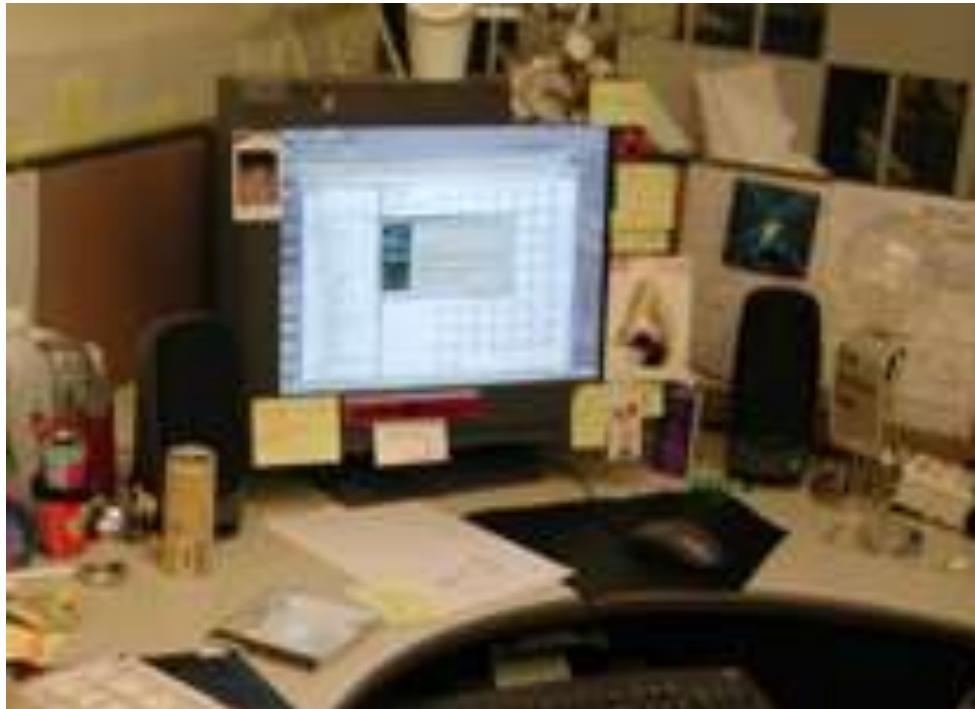
- Task Requirements
  - Remember 30 pseudo-random passwords
  - Change every other 3 months
  - No not take memo

Human cannot cope to security!



# HCI Issues: ID/PW

- Password authentication survey (HFES, 2009)
  - Users record on sticker 15-20%
  - Enterprise users record on notebooks (66%), computer file (55%)
- ※ 1% PW among 3,200 Million PW 1% 123456 (Imperva, 2010)



# HCI Issues: Security Patch

---

- Different perception between security and other update
  - Window update, security patch, agreement (20% compliance)
  - Game patch, no agreement (100% compliance)
- Automatic security patch downloads for Hangame
  - Advanced agreements for automatic patch
  - 200 million patch clients for 16days
- Users perception to security patch
  - Security is additional function, not key elements

# HCI Issues: i-PIN

- Difficult to change users behavior
  - SSN vs. i-PIN
  - Up to 8 Million copies from 2006
- High business risk in using SSN
  - Marking >>> Security
  - SKComs Case, \$2,000 compensation for each



# HCI Issues: PKI

- Enhancing technology not intrusive
  - Analogy to real world procedure
    - > Seal or signature for cyber banking
- Convenient and cost effective
  - Immediate money transaction
- When security is user values
  - Mandatory for cyber banking and trading



Users will accept additional cost, only if security is users value.

# HCI Issues: Complexity of Security Technology

- Complexity of System
  - Internal Complexity
  - External Complexity: Interface
- Complexity of security tech.
  - S/W: Vaccine, Anti-Spyware, etc.
  - H/W: F/W, IDS, Web F/W, IPS, etc.

RADIO CORPORATION OF AMERICA

OPERATING INSTRUCTIONS FOR AERIOLA SR.

Test numbers correspond with above diagram.

Numbers Corresponding to Diagram

No. 1. First, refer to accompanying sketch, then erect antenna and place protective device in position as described on page 56.

No. 2. Connect a wire leading from terminal marked R on protective device to binding post indicated by arrow for stations below 350 meters.

No. 3. For stations between 350 and 500 meters, connect the above wire to this post.

No. 4. Connect this post with terminal G of protective device.

No. 5. Connect telephone receivers to these two posts.

No. 6. Turn rheostat as far as it will go toward tail of arrow.

No. 11. Place "Tickler" pointer at zero point of scale.

No. 12. Turn rheostat (6) toward point of arrow until vacuum tube shows dull red. Do not try to burn too brightly as this materially reduces the life of the filament.

No. 13. Rotate tuning handle slowly over the scale, meanwhile listening until sound is heard in the telephone receivers. Adjust to best position, then increase "Tickler" (11) until maximum strength of signal is obtained. If tickler is turned too far toward maximum position, signals will lose their natural tone and reception of telephone signals may become difficult.

Note: This terminal is also connected to terminal G of the protective device.

Complete Aeriola Sr. Broadcasting Receiver, Model RF, 190-500 Meters, with One Aeriontron WD-11-D Vacuum Tube, One Filament Dry Cell, One Plate Dry Battery, Head Telephone Receivers, Antenna Equipment and Full Instructions. \$75.90

Aeriola Sr. Broadcasting Receiver, Model RF, As Above, Less Batteries and Antenna Equipment. \$65.00

Dimensions: 7 in. x 8½ in. x 7¾ in.

Weights: Net, 6 lbs.; Shipping, 12 lbs.; with Antenna Equipment and Batteries, 25 lbs.

NOTE: For Prices of other Complete Receiver Combinations, see page 18.

# HCI Issues: Culture and Environments

---

- Difficult to change culture, infra
  - Easy to adopt a new technical change, difficult to change business practice and culture
  - SSN is widely used for Internet Business
  - > e.g.) New standards for Industry: Km, m<sup>2</sup>
- Technology influences our culture
  - Privacy in using telephone in 1800s
  - Smartphone?

# Usability Design for Information Security

---

- Bias perception of risk (Tversky and Kahneman, 1973)
  - overestimate the value of their own experience if they have not been exposed, underestimate the risk
  - overestimate the associate with news stories
- “It can’t happen to me” bias (Christensen, 1987)
  - Overconfident of their ability to avert accident e.g., 75–90% believe they are above average in driving skill
- People will accept a higher level of risk (Slovic, 1978)
  - if the level of risk is controllable, is known, and understood, and the consequence are immediate

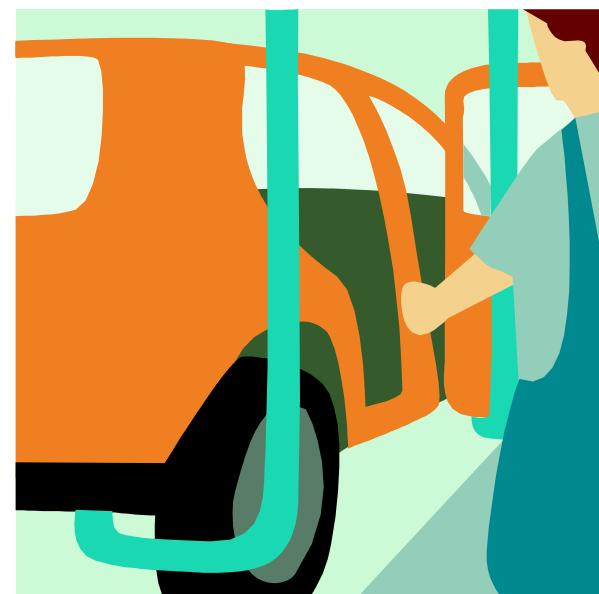
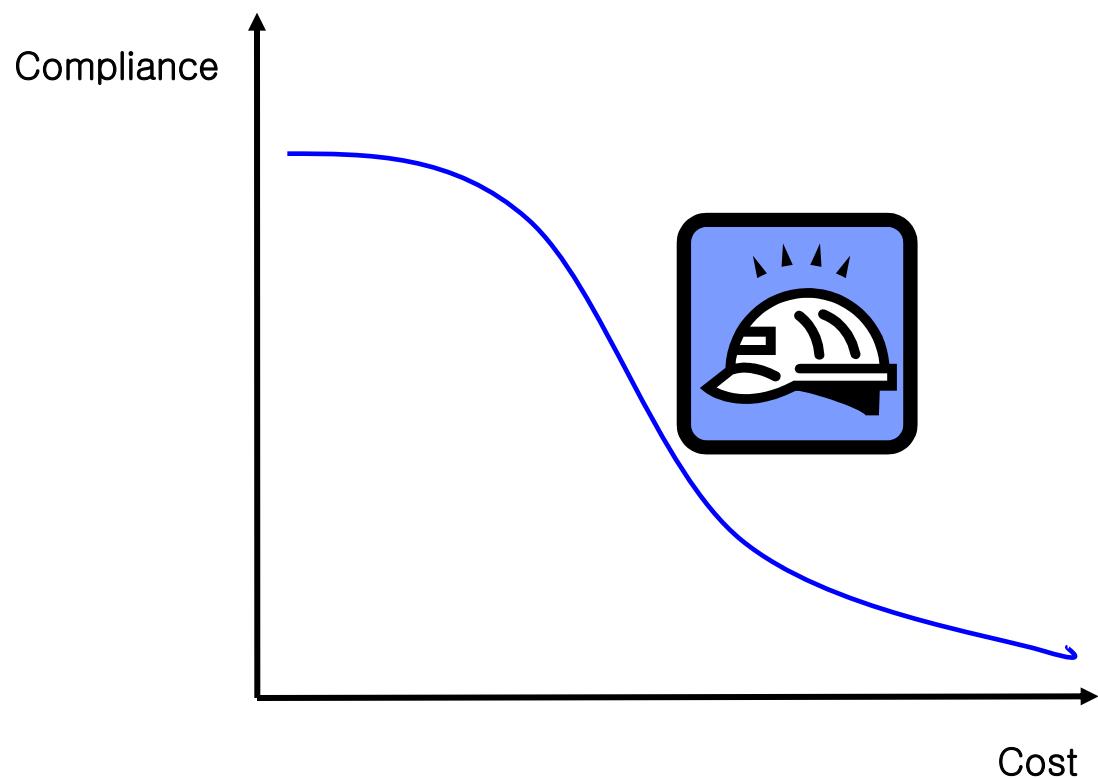
# Mental Model

- Explanation of one's thought process about how something works in the real world



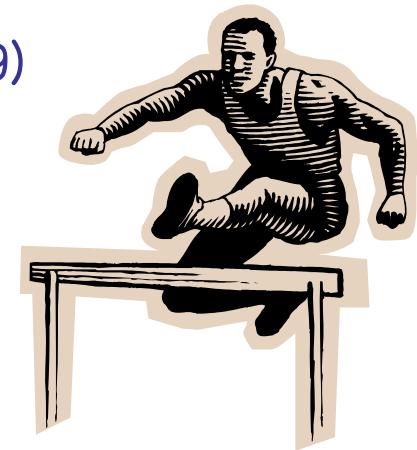
# Cost of Compliance

- User will not use if the cost of compliance is high
  - Cost, effort, time etc.



# Usability Design for Information Security

- New security technology will improve the level of security?
  - Cannot be without transforming the weakest link
  - > User-Centered Design for Security Mechanism
  - ※ 84% of Security Failure, Human Error (Deloitte, 2009)
- HCI
  - Information security is man-machine System
  - Trade-Off between usability and security
  - Need to understand users and their tasks



Security is only as good as its weakest link,  
and people are the weakest link in the chain