Usability and Psychology

Usability and Psychology

Humans are incapable of securely storing high-quality cryptographic keys…performing cryptographic operations

— Kaufmann, Perlman and Speciner

Only amateurs attack machines; professionals target people.

— Bruce Schneier

Introduction

- Real attacks exploit psychology
  - Phishing
  - Easy to do and hard to stop
- Social engineering
  - E.g., Steve Jobs Heart-Attack Hoax
- Understand what works and why

Attacks

Attacks Based on Psychology

- Pretexting
  - 30 false-pretext calls/week for a district of 250,000 people in UK
- Phishing
  - Harder for companies, targeted on customers
  - Losses are growing rapidly, average 10,000-employee company spends $3.7 million in 2015

Insight

Insight from Psychology Research

- Security and psychology will be a big research area
- Attackers target at users instead of technology
- Psychology is a huge subject

Brain vs. Computer

- Using cognitive psychology
  - No. of menu items
- HCI, including perception, motor control, memory and problem solving

Human errors

- Slips and lapses at the level of skills
  - Inattention causes a practiced action to be performed instead of an intended one
  - E.g., click “OK” button
  - E.g., leave ATM card behind in ATMS
- Mistakes at the level of rules
  - Follow wrong rules, https://
- Mistakes at the cognitive level

Perceptual Bias & Behavioral Economics

- Study heuristics the people use
- The biases that influence people
- People's decision processes depart from the rational behavior models

More on Insight

What is Your Choice

- Example 1
  - Get $1M for sure
  - Get $2M 50%
- Example 2
  - Lose $100 for sure
  - Lose $200 50%

Prospect Theory

- Make decisions with uncertainty
- Risk aversion
- People are bad at calculating probability
  - We based inferences on familiar or easily-imagined analogies
  - The channels that we experience things

Perception and Irrational

- Perception of risk
  - Food poisoning vs. terrorism
- Biased to thing that we are in control
  - Driving a car vs. taking an plane

Passwords

Passwords

- An instructive example of usability, applied psychology, and security
- Worst authentication mechanism!?
- Outsiders guessing
- Insiders in other systems know
- Identity theft, half million in USA every year

Difficulties

- Reliable entry
  - Not too long
  - Not too complex
  - E.g., reservation numbers, electricity meters in South Africa
- Remembering passwords
  - Most people choose passwords that are easy for attackers to guess
  - They write them down

Naïve Password Choice

- Simple passwords
  - Spouses' names, single letters, carriage return
- Force password to be at least six characters long
  - Common names + number
- Require change passwords regularly
  - Change password rapidly
- Forbid to change password in 15 days
  - Favorite password + month

Password Checking + Training

- A good password selection approach
  - Effective (difficult to guess)
  - Relatively easy to remember
- User compliance
  - Based on applications

Lessons Learned

Lessons Learned

- Design errors
  - Use mother's maiden name
  - Password reuse (e.g. PIN numbers)
- Operational issues
  - Display passwords
  - Fail to reset default passwords

Social Engineering Attacks

- The core problem of phishing: disclosing the password to a third party
  - Accident or result of deception, e.g. pretexting
- Strict policies
  - E.g., Sun Microsystems' root password
  - Do not click on links in emails
  - Do not give security information over the phone
- Still many problems
  - E.g., PayPal, Citibank, BoA's emails to customers

Trusted Path

- Being sure to interact with a genuine machine
  - Fake login screen
  - Secure attention sequence Ctrl-alt-del
  - Crooked cash machine or even bank branch

CAPTCHA

CAPTCHA and ReCAPTCHA

- Use the brain's strengths rather than its weaknesses
- Came in 2003
- Use a known 'hard problem' in AI
  - The recognition of distorted text against a noisy background
  - Turned out not to be too hard
  - Spammers created a game and solving one CAPTCHA after another
- ReCAPTCHA, 2014
  - Users solve problems that confused OCR and check their answers against each other

Phishing Countermeasure

Phishing Countermeasures (1)

- Password mangler
  - Hash(password + secret key + domain name)
  - Practical problems (e.g. syntax may be different for different websites)
- Client certificates
  - SSL + client certificate

Phishing Countermeasures (2)

- Browser's password database
  - The benefit of a password mangler
  - Might be compromised from malware
  - If autocomplete is turned off, phishing detect is turned off
- Soft keyboards
  - Display keyboard on screen
  - Attackers capture the screen around each mouse click

Phishing Countermeasures (3)

- Customer education
  - Ask customers to follow rules
    - Check the English
    - Lock symbol
  - Become more and more counterintuitive and complex
- Microsoft passport
  - Using Hotmail account + Kerberos
  - Problems: privacy, dominant position

Phishing Countermeasures (4)

- Phishing alert toolbars
  - Check for wicked URLs
  - ‘Picture-in-picture’ website
- Two-factor authentication
  - Security tokens produce one-time password
  - Password + eight digits (function of time)
  - Attackers may use man-in-the-middle attack

Phishing Countermeasures (5)

- Trusted computing
  - Security chips in PC motherboards
  - Not there yet
- Two-channel authentication
  - Password + a code from another channel (e.g. cell phone)
  - Assumption of independence (may break down if everyone use Internet via phones)
  - Usability issue might cost companies
  - Man-in-the-middle attack

Other Phishing Attacks Targets

- Attacks
  - Target may change from banks to suppliers
  - Bad guys may match the context of their phish
  - More man-in-the-middle attacks
  - Bad companies buy ads from websites such as Google
- Countermeasures
  - Two-factor authentication
  - Extra authentication for the first time

Key Points

Key Points

- Usability
- Attacks based on psychology
- Insight from psychology research
- Passwords and lessons learned
- Phishing attacks and countermeasures