Security Engineering

Psychology and Behavioural Economics

Social Engineering

- Use a plausible story, or just bully the target
- 1980s: ‘What’s your PIN so I can cancel your card?’
- Threat to students: don’t get phished into acting as money mules!
- Many attacks on companies and governments...
- Organisational defence: control external communications, and limit the harm that any one person or machine can do
  - mandatory access control
  - operational security

Scaling it up: phishing

- Took off in 2006, when UK banks lost £35m (£33m by one bank) and US banks maybe $200m
- Lures evolve
  - ‘Thank you for adding a new email address to your PayPal account’
  - ‘This is NHS Test and Trace’
- Can be combined with tech exploits, e.g. caller ID spoofing
- Pervasive – 80% of UK adults targeted last year (many for other scams but still...)

Spear phishing nowadays

- The Snooping Dragon (2008) – China vs Tibetans
- Now it's one of the main techniques used in both ransomware and cyberwar
- A well-crafted, personalised lure can get 30% yield
- Some big consequences, e.g. John Podesta in 2016
- Banks, intel agencies, tech companies protect staff by two-factor authentication, mail filtering etc
- Spooks go for political campaigners, journalists; ransomware gangs for hospitals, ordinary firms

Psychology of safety and security

- Errors arise at different levels of the ‘stack’
  - We deal with novel problems in a conscious way
  - Frequently encountered problems are dealt with using rules we evolve, and are partly automatic
  - Over time, the rules give way to skill
- Our ability to automatise routine actions leads to absent-minded slips, or following a wrong rule
- There are also systematic limits to rationality – ‘heuristics and biases’, as well as social psychology
- This gives us a rough taxonomy of errors

Error types

- Knowledge-based (and ignorance-based) mistakes
- Processing biases, based on how human brains work
- Rule-based mistakes: applying wrong procedure
- Slips and lapses
  - Forgetting plans, intentions; habit intrusion
  - Premature exits from action sequences, e.g. ATMs
  - Misidentifying objects, signals (often Bayesian)
  - Retrieval failures; tip-of-tongue, interference

Social psychology

- Conformity: Solomon Asch showed most people would deny obvious facts (like relative line length) to conform with others
- Authority: Stanley Milgram showed that over 60% of all subjects would inflict a potentially fatal shock on a ‘student’ if ordered to do so by a ‘teacher’
- Philip Zimbardo’s Stanford Prison Experiment suggested that roles alone might be enough!

The social brain hypothesis

- Old view: we got smart to make better tools
- Archaeology: we got smart first!
- New view: when Africa dried out 1.5m years ago, we started living in bigger groups
- Primate brain size correlates well with group size
- Social aspect: big brains track more relationships
- Machiavellian aspect: if you're better at deception, and at detecting deception in others, you're more likely to have descendants

Gender

- Men are much more likely to commit crime!
- Particularly low-status men with issues about their gender role or place in social hierarchy
- Most terrorists, mass shooters commit violent crime against women first
- Misogyny is strongly linked to alt-right movement; see Gamergate
- Links to cybercrime too

Social Psychology and Marketing

- Reciprocation can be used to draw people in (even monkeys to tit-for-tat)
- Use social proof: people like to do what others do
- They buy from people they can relate to
- They also like to defer to authority
- Get a commitment and follow through (people want to be consistent)
- See Cialdini's "Influence – Science and Practice"

Context and Framing

- Framing effects include the estate agent who shows you a crummy house first
- Take along an ugly friend on a double date …
- Get user fixated on task completion (e.g. finding why there's suddenly a new payee on your PayPal account)
- Advance fee frauds take this to extreme lengths!
- Risk salience is hugely dependent on context! E.g. CMU experiment on privacy

Fraud psychology

- All the above plus
  - Appeal to the mark's kindness
  - Appeal to the mark's dishonesty
  - Distract them so they act automatically
  - Arouse them so they act viscerally
- See "The Real Hustle" videos on YouTube
- For the gory details, see Modic and Lea, or Kevin Mitnick's 'Art of Deception'

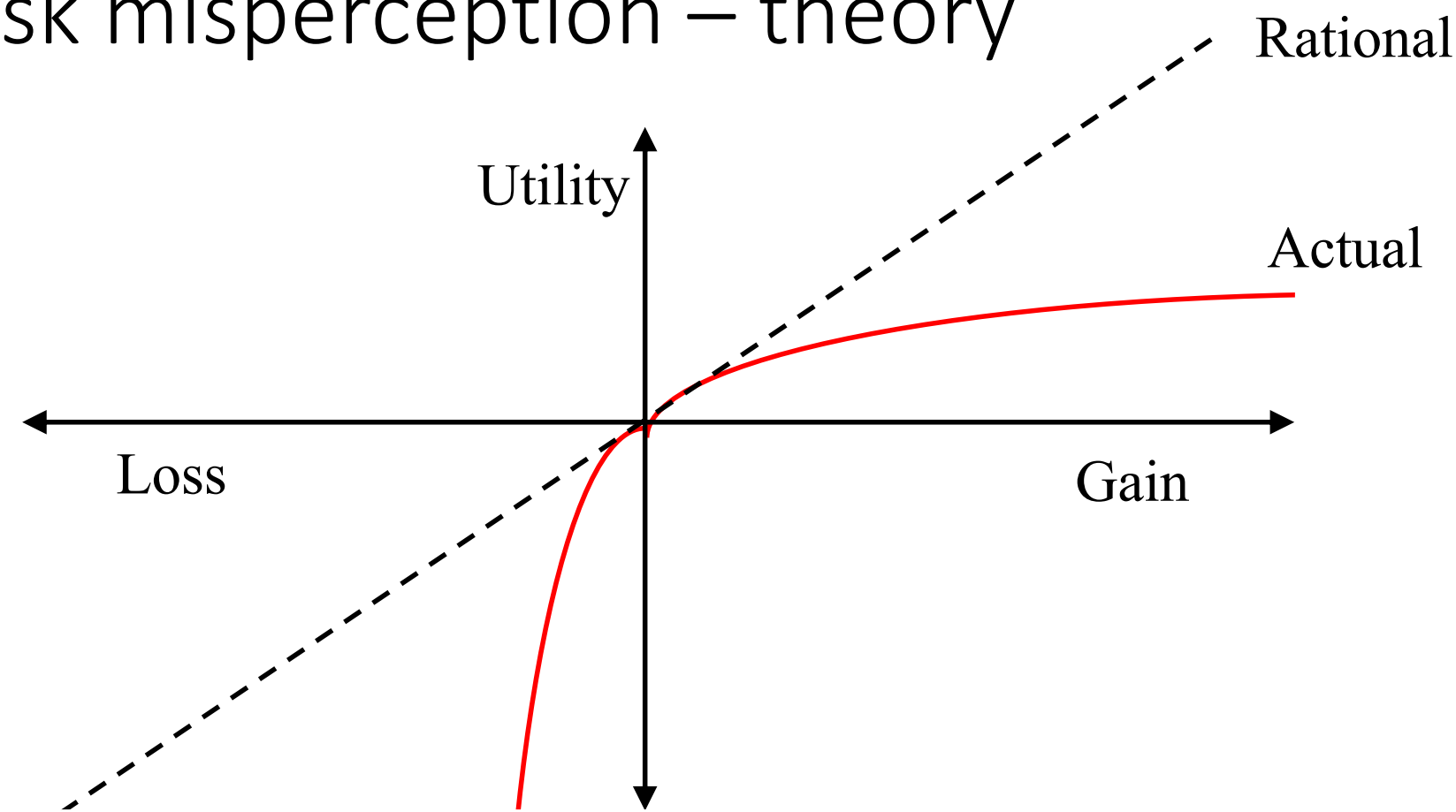
Economics versus psychology

- Most people don’t worry enough about computer security
- How could this be fixed, and why is it not likely to be?
- Most people worry too much about terrorism
- How could this be fixed, and why is it not likely to be?

Behavioural economics

- People make buying decisions with the emotions and rationalise afterwards
- Mostly we're too busy to research each purchase – and in the ancestral evolutionary environment we had to make flight-or-fight decisions quickly
- The older parts of the brain kept us alive for millions of years before we developed analytical thought (see Kahneman, "Thinking Fast and Slow")
- Their reflexes appear in mental shortcuts such as quality = price and quality = scarcity

Risk misperception – theory



People offered £10 or a 50% chance of £20 usually prefer the former; if offered a loss of £10 or a 50% chance of a loss of £20 they tend to prefer the latter!

Framing decisions about risk

- Decisions are heavily influenced by framing. E.g. the ‘Asian disease problem’ where the subject is making decisions on vaccination. Two options put to subjects. First:

  A: “200,000 lives will be saved”

  B: “with p=1/3, 600,000 saved; but p=2/3 none saved”
- Here 72% choose A over B!
- Second option is

  C: “400,000 will die”

  D: “with p =1/3, no-one will die, p=2/3, 600,000 die”
- Here 78% prefer D over C!
- This is also why marketers talk ‘discount’ or ‘saving’ – and fraudsters know that people facing losses take more risks

Risk misperception – practice

- Why do we overreact to terrorism?
  - Risk aversion / status quo bias
  - ‘Availability heuristic’ – easily-recalled data used to frame assessments
  - Our behaviour evolved in small social groups, and we react against the out-group
  - Mortality salience greatly amplifies this
  - We are also sensitive to agency, hostile intentions
  - Terrorists maximise the threat; police & politicians too
- See book chapters 2, 24

Usability for employees

- ‘Blame and train’ is not the best approach!
- People will spend only so much time obeying rules – the compliance budget – so understand it, and choose the rules that matter
- Rule violations are often an easier way of working, and sometimes necessary, so watch them, measure them and adapt to them
- The ‘right’ way of working should be easiest; the defaults should be safe

Usability for the public: defaults

- What actions do you make natural?
- Most people won't opt in, or opt out; they go with the default
  - Governments try to set socially optimal defaults (e.g. you must opt out of pensions)
  - Facebook privacy settings: advertiser-friendly?
- Where else do private incentives clash with public goods?

Where should the path be?

Affordances: Johnny Can’t Encrypt

Why Johnny Can’t Encrypt:
A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar[1]
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

Abstract

User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to apply standard user interface design techniques to security? We argue that, on the contrary, effective security requires a different

1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the encrypt button when they need privacy, give up on a communication protocol because they are too confused

Users' mental models

- Explore how your users see the problem – the 'folk beliefs'
  - threats seen as 'viruses' which could be mischievous, or crime tools;
  - 'hackers' who may be seen as graffiti artists or burglars or targeting big fish;
  - Or simply as 'bad neighbourhoods' online!
- People are more likely to follow security advice consistent with their mental model

Passwords

- Cheapest way to authenticate, but 3 issues:
  - Will users enter passwords correctly?
  - Will they remember them, or will they choose weak ones or write them down?
  - Can they be tricked into revealing them?
- Advice is often like ‘choose something you can’t remember and don’t write it down’
- We know lots about password / PIN design failures! See SE chapter 3 for more

Externalities

- One firm’s action has side-effects for others
- Password sharing a conspicuous example
- Bulk password compromise is too common
- Everyone wants recovery questions too (and can leak them by the million when hacked)
- Firms train customers in unsafe behaviour such as clicking on external links
- Much ‘training’ amounts to victim blaming

Usability for developers

- Many security bugs are due to tools that are too hard to use safely
  - The C programming language
  - Crypto APIs that default to electronic code book mode (including MS and Arm offerings)
- Many more arise when busy programmers copying insecure code snippets from online forums
- Usability for developers is now the most rapidly-growing area of security usability research and practice!