Towards a Science of Security and Human Behaviour

Ross Anderson
Cambridge University

Traditional View of Infosec

- People used to think that the Internet was insecure because of lack of features – crypto, authentication, filtering
- So we all worked on providing better, cheaper security features – AES, PKI, firewalls …
- About 1999, some of us started to realize that this is not enough

Economics and Security

- Since 2000, we have started to apply economic analysis to IT security and dependability
- It often explains failure better!
- Electronic banking: UK banks were less liable for fraud, so ended up suffering more internal fraud and more errors
- Distributed denial of service: viruses now don't attack the infected machine so much as using it to attack others
- Why is Microsoft software so insecure, despite market dominance?

New View of Infosec

- Systems are often insecure because the people who guard them, or who could fix them, have insufficient incentives
  - Bank customers suffer when poorly-designed bank systems make fraud and phishing easier
  - Casino websites suffer when infected PCs run DDoS attacks on them
- Insecurity is often what economists call an 'externality' – a side-effect, like environmental pollution

New Uses of Infosec

- Xerox started using authentication in ink cartridges to tie them to the printer – and its competitors soon followed
- Carmakers make ‘chipping’ harder, and plan to authenticate major components
- DRM: Apple grabs control of music download, MS accused of making a play to control distribution of HD video content

IT Economics (1)

- The first distinguishing characteristic of many IT product and service markets is network effects
- Metcalfe's law – the value of a network is the square of the number of users
- Real networks – phones, fax, email
- Virtual networks – PC architecture versus MAC, or Symbian versus WinCE
- Network effects tend to lead to dominant firm markets where the winner takes all

IT Economics (2)

- Second common feature of IT product and service markets is high fixed costs and low marginal costs
- Competition can drive down prices to marginal cost of production
- This can make it hard to recover capital investment, unless stopped by patent, brand, compatibility …
- These effects can also lead to dominant-firm market structures

IT Economics (3)

- Third common feature of IT markets is that switching from one product or service to another is expensive
- E.g. switching from Windows to Linux means retraining staff, rewriting apps
- Shapiro-Varian theorem: the net present value of a software company is the total switching costs
- So major effort goes into managing switching costs – once you have $3000 worth of songs on a $300 iPod, you're locked into iPods

IT Economics and Security

- High fixed/low marginal costs, network effects and switching costs all tend to lead to dominant-firm markets with big first-mover advantage
- So time-to-market is critical
- Microsoft philosophy of ‘we’ll ship it Tuesday and get it right by version 3’ is not perverse behaviour by Bill Gates but quite rational
- Whichever company had won in the PC OS business would have done the same

IT Economics and Security (2)

- When building a network monopoly, you must appeal to vendors of complementary products
- That's application software developers in the case of PC versus Apple, or now of Symbian versus Linux/Windows/J2EE/Palm
- Lack of security in earlier versions of Windows made it easier to develop applications
- So did the choice of security technologies that dump usability costs on the user (SSL, not SET)
- Once you've a monopoly, lock it all down!

Economics and Usability

- Make your products usable by newbies
- … but much more usable with practice!
- To what extent can you make skill a source of asymmetric lockin?
- Hypothesis: this underlies the failure of user programmability to get traction!
- We have nothing now as good as BASIC was in the 1980s…

Economics and Usability (2)

- How many features should my product have?
- Marginal benefit of new feature concentrated in some target market
- Marginal cost spread over all users
- So we get chronic featuritis!
- At equilibrium, a computer / phone / anything programmable will be just on the edge of unacceptability to a significant number of users
- The same happens with laws, services, …

Why are so many security products ineffective?

- Akerlof's Nobel-prizewinning paper, 'The Market for Lemons' introduced asymmetric information
- Suppose a town has 100 used cars for sale: 50 good ones worth $2000 and 50 lemons worth $1000
- What is the equilibrium price of used cars?
- If $1500, no good cars will be offered for sale …
- Started the study of asymmetric information
- Security products are often a 'lemons market'

Products worse then useless

- Adverse selection and moral hazard matter (why do Volvo drivers have more accidents?)
- Application to trust: Ben Edelman, ‘Adverse selection on online trust certifications’ (WEIS 06)
- Websites with a TRUSTe certification are more than twice as likely to be malicious
- The top Google ad is about twice as likely as the top free search result to be malicious (other search engines worse …)
- Conclusion: ‘Don’t click on ads’

Privacy

- Most people say they value privacy, but act otherwise. Most privacy ventures failed
- Why is there this ‘privacy gap’?
- Odlyzko – technology makes price discrimination both easier and more attractive
- Acquisti et al – people care about privacy when buying clothes, but not cameras (phone viruses worse for vendor than PC viruses?)
- Loewenstein et al – it’s not clear that there are stable and coherent privacy preferences! Student disclosure more for ‘How bad RU’ and less with detailed privacy notice

Conflict theory

- Does the defence of a country or a system depend on the least effort, on the best effort, or on the sum of efforts?
- The last is optimal; the first is really awful
- Software is a mix: it depends on the worst effort of the least careful programmer, the best effort of the security architect, and the sum of efforts of the testers
- Moral: hire fewer better programmers, more testers, top architects

How Much to Spend?

- How much should the average company spend on information security?
- Governments, vendors say: much much more than at present
- But they've been saying this for 20 years!
- Measurements of security return-on-investment suggest about 20% p.a. overall
- So the total expenditure may be about right. Are there any better metrics?

Skewed Incentives

- Why do large companies spend too much on security and small companies too little?
- Research shows an adverse selection effect
- Corporate security managers tend to be risk-averse people, often from accounting / finance
- More risk-loving people may become sales or engineering staff, or small-firm entrepreneurs
- There's also due-diligence, government regulation, insurance and agency to think of

Skewed Incentives (2)

- If you are DirNSA and have a nice new hack on XP and Vista, do you tell Bill?
- Tell – protect 300m Americans
- Don't tell – be able to hack 400m Europeans, 1000m Chinese,…
- If the Chinese hack US systems, they keep quiet. If you hack their systems, you can brag about it to the President
- So offence can be favoured over defence

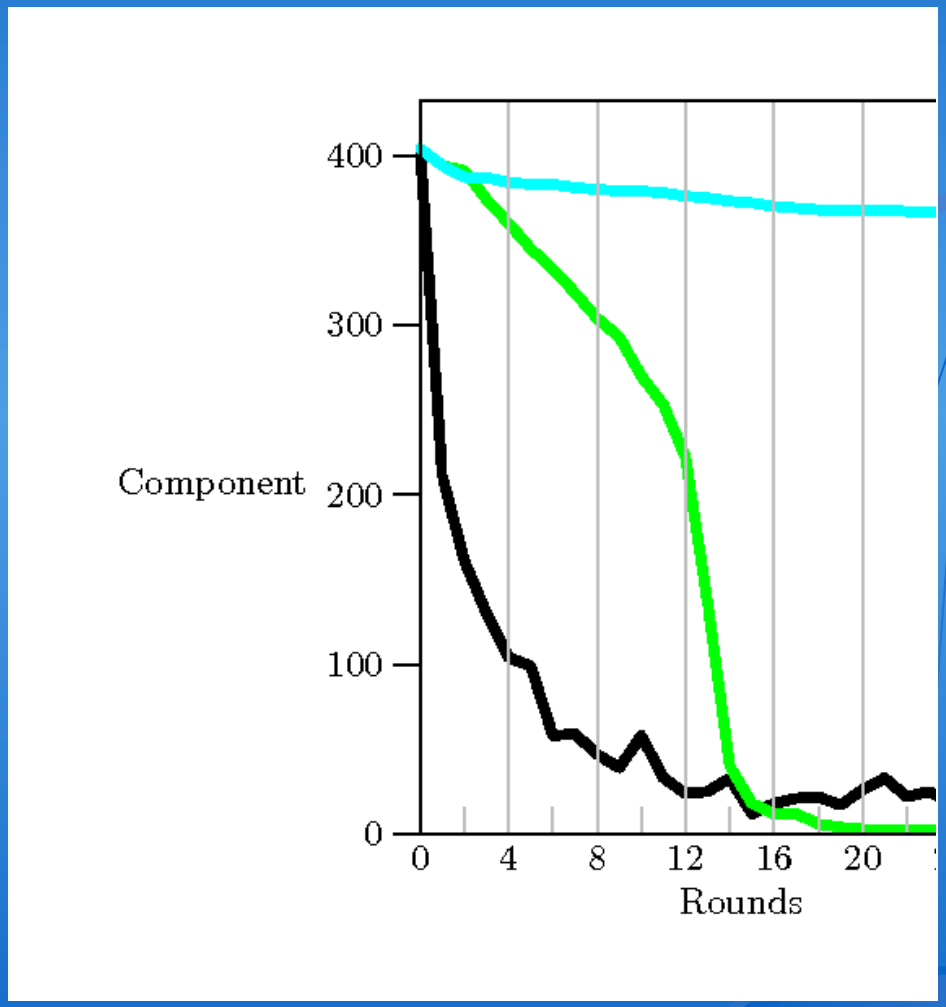
Security and Policy

- Our ENISA report, published in March, has 15 recommendations:
  - Security breach disclosure law
  - EU-wide data on financial fraud
  - Data on which ISPs host malware
  - Slow-takedown penalties and putback rights
  - Networked devices to be secure by default
  - …
- See links from my web page

Security and Sociology

- There's a lot of interest in using social network models to analyse systems
- Barabási and Albert showed that a scale-free network could be attacked efficiently by targeting its high-order nodes
- Think: rulers target Saxon landlords / Ukrainian kulaks / Tutsi schoolteachers /…
- Can we use evolutionary game theory ideas to figure out how networks evolve?
- Idea: run many simulations between different attack / defence strategies

Security and Sociology (2)



Vertex-order attacks with:

- Black – normal (scale-free) replenishment
- Green – defenders replace high-order nodes with rings
- Cyan – they use cliques (c.f. system biology …)

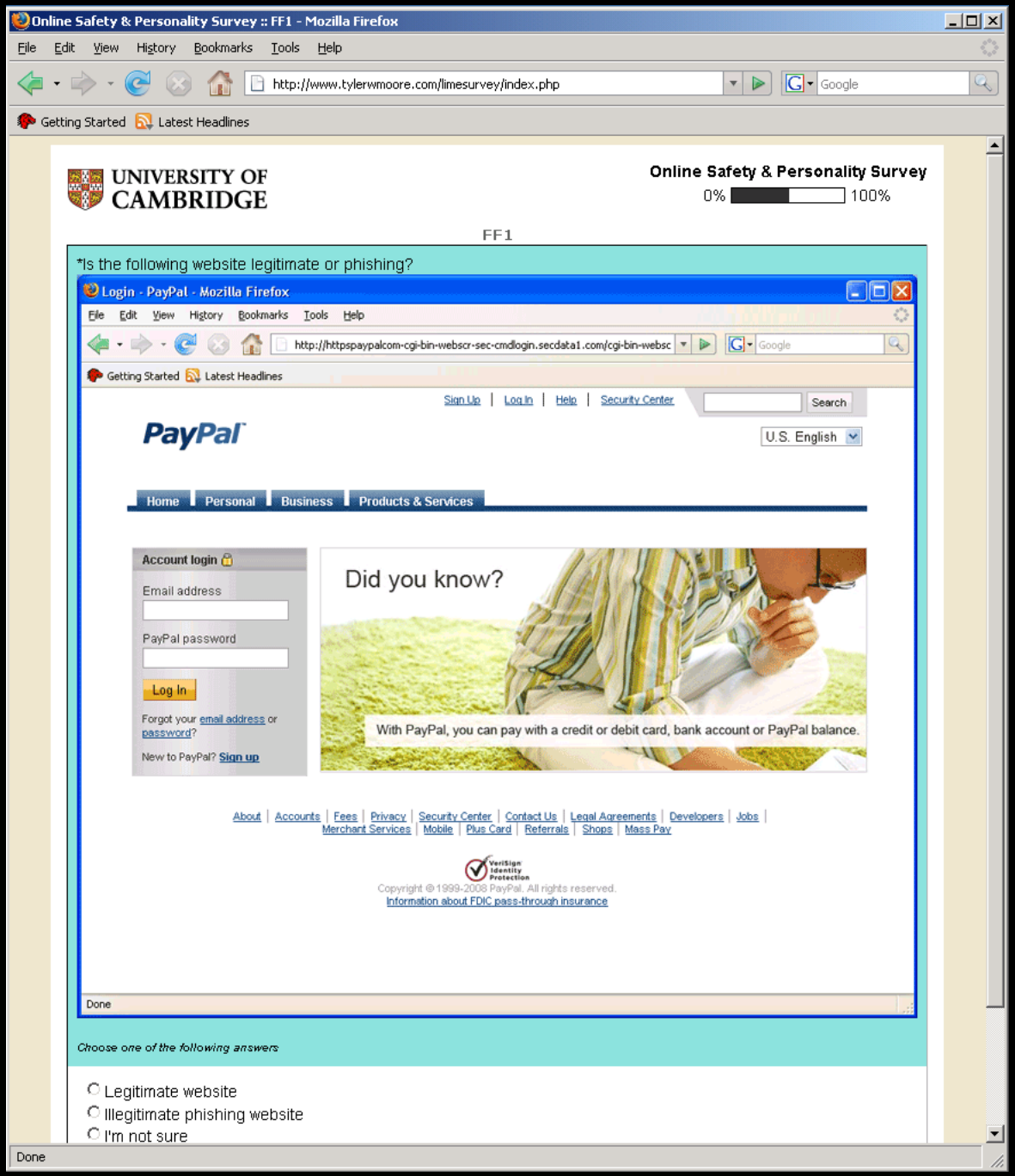
Application: traffic analysis (see my Google tech talk)

Psychology and Security

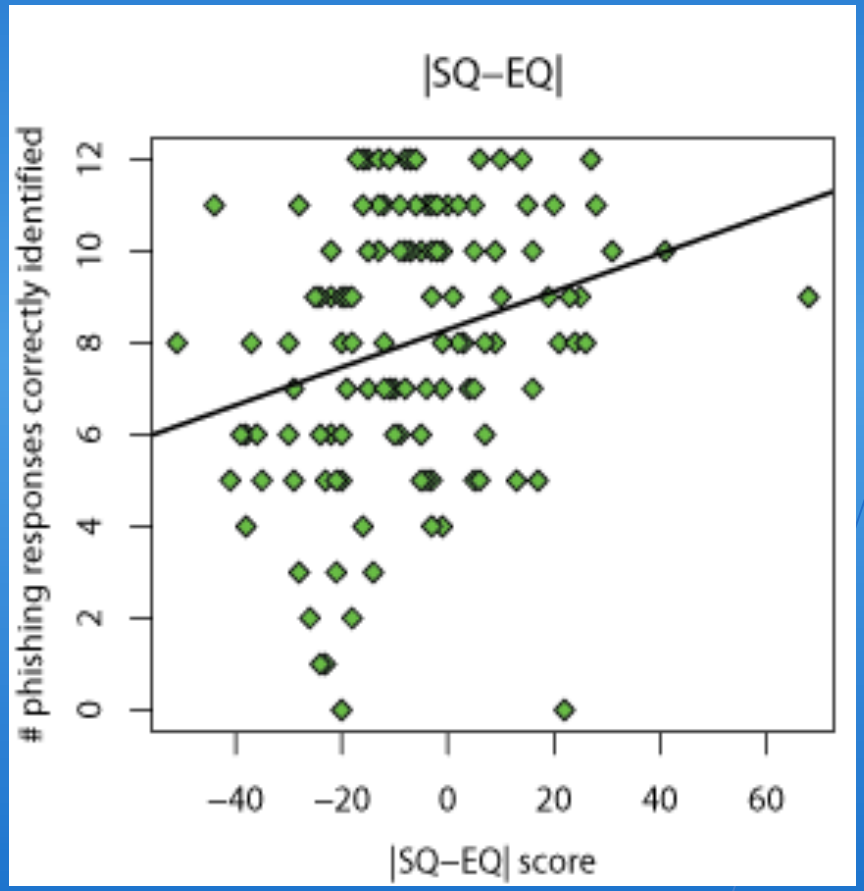
- Phishing only started in 2004, but in 2006 it cost the UK £35m and the USA perhaps $200m
- Banks react to phishing by ‘blame and train’ efforts towards customers
- But we know from the safety-critical world that this doesn’t work!
- We train people to keep on clicking ‘OK’ until they can get their work done – and ‘learned helplessness’ goes much wider
- People don’t notice missing padlock – the ‘dog that didn’t bark’. Is there anything we can do?

Psychology and Security (2)

- Folklore: systems designed by geeks for geeks also discriminate against women, the elderly and the less educated
- We set out to check whether people with higher ‘systemizing’ than ‘empathizing’ ability would detect phishing more easily
- Methodology: tested students for phishing detection, and also on Baron-Cohen test
- Presented at SHB07: re-examined by sex


Online Safety & Personality Survey :: FF1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.tylerwmoore.com/limesurvey/index.php
Getting Started Latest Headlines
UNIVERSITY OF CAMBRIDGE
Online Safety & Personality Survey
0% 100%
FF1
*Is the following website legitimate or phishing?
Login - PayPal - Mozilla Firefox
http://httpspaypalcom-cgi-bin-webscr-sec-cmdlogin.secdata1.com/cgi-bin-websc
Sign Up | Log In | Help | Security Center
Search
PayPal
U.S. English
Home Personal Business Products & Services
Account login
Email address
PayPal password
Log In
Forgot your email address or password?
New to PayPal? Sign up
Did you know?
With PayPal, you can pay with a credit or debit card, bank account or PayPal balance.
About | Accounts | Fees | Privacy | Security Center | Contact Us | Legal Agreements | Developers | Jobs | Merchant Services | Mobile | Plus Card | Referrals | Shops | Mass Pay
Copyright © 1999-2008 PayPal. All rights reserved.
Information about FDIC pass-through insurance
Done
Choose one of the following answers
Legitimate website
Illegitimate phishing website
I'm not sure
Done

Results



- Ability to detect phishing is correlated with SQ-EQ
- It is (independently) correlated with gender
- Folklore is right – the gender HCI issue applies to security too

Psychology and Security (3)

- Social psychology has long been relevant to us!
  - Solomon Asch showed most people would deny the evidence of their eyes to conform to a group
  - Stanley Milgram showed that 60% of people will do downright immoral things if ordered to
  - Philip Zimbardo's Stanford Prisoner Experiment showed roles and group dynamics were enough
- The disturbing case of 'Officer Scott'
- How can systems resist abuse of authority?

Psychology and Security (4)

- Why does terrorism work?
- The bad news: it's evolved to exploit a large number of our heuristics and biases!
- Availability heuristic; mortality salience; anchoring; loss aversion in uncertainty; wariness of hostile intent; violation of moral sentiments; credence given to images; reaction against out-group; sensitivity to change;…
- The good news: biases affect novel events more, and so can be largely overcome by experience

Psychology and Security (5)

- Deception – from its role in evolution, to everyday social poker; self-deception; how deception is different online, and policy…
- Would you really vote for a president you didn't think could lie to you?
- Many inappropriate psychological 'interfaces' are sustained by money or power – compare why we fear computer crime too little, and terrorism too much

The Research Agenda

- The online world and the physical world are merging, and this will cause major dislocation for many years
- Security economics gives us some of the tools we need to understand what's going on
- Sociology gives some cool and useful stuff too
- And security psychology is not just usability and phishing – it might bring us fundamental insights, just as security economics has

More …

- See www.ross-anderson.com for a survey article, our ENISA report, my security economics resource page, and links to:
- WEIS – Annual Workshop on Economics and Information Security
- SHB – Workshop on Security and Human Behaviour (www.lightbluetouchpaper.org)
- 'Security Engineering – A Guide to Building Dependable Distributed Systems' 2e – just out!


WILEY
Security Engineering
Ross Anderson
SECOND EDITION
A Guide to Building Dependable Distributed Systems