Personal Internet Security

Dr Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

House of Lords
Science & Technology
Select Committee

Briefing, 2 Nov 2006

Summary

- What’s the problem ?
- What’s the cause ?
- What’s the solution ?

Problems : losing money

- “Phishing”, and other con tricks by email
  - even experts can be unsure of validity of email
- “419” advanced fee fraud
  - affects the greedy (so why bother policing?)
- Fake lotteries
  - affects the gullible & naïve (so should protect?)
- Fraud
  - fake auctions, fake escrow sites, fake products

Problems : losing identity

- Loss of personal details
  - keyloggers, disk scanning, genealogy websites, insecure merchants (+phishing+419) etc etc
  - can be the precursor to extremely serious fraud, involving mortgages, loans &c
  - often very time consuming to correct (and "defamatory" statements can remain on file)
- NB: "identity theft" figures often contaminated by "card not present" fraud

Problems : losing control

- Spyware/Adware – unexpected pop-ups
- Viruses – install keyloggers & backdoors
- Spam – wastes time and resources
- Botnets
  - your “zombie” machine joins criminal army
- VoIP not quite like POTS
  - 999 doesn’t necessarily work

Problems: personal safety

- Bullying, harassment, stalking
- “Grooming” of children
  - Met putting significant resources into this
- Inappropriate content for children
  - no “top shelf” on the Internet (labelling is rare)
- Inappropriate content for anybody
  - illegal images of children, “extreme” pornography, bomb-making, drugs, gambling, stalking, defamation…

Metrics?

- Very few published figures about anything
  - don't want to affect stock price
  - eCrime doesn't figure in Home Office targets
- Few agreed definitions on measuring
- Many measurements done at a fixed point
  - spam filterers report what they discard, but do the spammers (possibly only 200 of them) take any steps to avoid sending to them ?
  - does your spam look like mine ?

Many other issues

- Security of mobile phones
  - address books and other personal data
  - theft of service
- Security of WiFi
  - theft of service
  - “framing” the innocent
- Security of iPods, data theft from RFID passports, and will even your toaster be safe?

Causes #1

- Operating System programmers
  - negligently shipping before finding all bugs
- Applications programmers
  - not paying enough (any?) attention to security
- System users (local and remote)
  - not bothering to find and apply patches
- Computer shops
  - selling unpatched software & not supporting users

Causes #2

- ISPs
  - not providing security for end-users
- Hardware manufacturers
  - not providing “secure-by-default” PCs, WiFi etc
- Regulators
  - not addressing “market failures”
  - not setting minimum security standards

Causes #3

- Criminals
  - doing bad things
- Police
  - not bothering (much) to catch them
- Legislators
  - not providing suitable laws
- Foreign Office
  - not making sure overseas crooks are dealt with

Causes #4

- End-users
  - not staying out of “bad neighbourhoods”
- Educators (DfES, OFCOM, BBC etc)
  - not teaching “media literacy”
- Banks
  - not giving customers security devices
- Businesses
  - not keeping personal data secure

Causes #5

- And many many more!
  - Sony debacle : DRM system compromised users
  - Titan rain : Chinese spies
  - Witty worm : escaped cyberwar software ?

Solutions: not really ☹

- "1p per email" to eliminate spam
  - complex to roll out & still leaves spam for Rolls Royces and fake (higher profit margin) pills plus provides yet another driver for theft of service
- Biometrics
  - unsuitable for unattended operation
- Two-factor authentication (etc)
  - doesn't address "man-in-the-middle" attack

Solutions : panaceas ☹

- Education
  - but you need to know an awful lot to be truly safe
  - bad guys exploit simple “rules of thumb”
  - most con-tricks are centuries old
- Firewalls (rule-based connection blocking)
  - stop bad incoming packets, but what’s “bad”?
- Anti-Virus software (scanning for bad stuff)
  - only works on mass-deployed viruses
  - “trusted computing” may obstruct AV

Solutions: policing

- NHTCU rolled up into SOCA and special funding of “Network Investigators” ceased
- Police strategy moving to “mainstreaming”
  - but must also address intelligence (is this tip of the iceberg?), cross-border crime and need for some specialist knowledge of methods used
  - “If it’s illegal offline then it’s illegal online” doesn’t illuminate questions of speed and automation (what network engineers call “scale”)

Solutions: a way forward ☺

- Avoid specific rules, but fix the incentives
  - force banks to carry losses for fraud ?
  - loss of personal data must be reported ?
  - shops must declare age of software images ?
  - advertisers responsible for spam/spyware ?
  - decouple VoIP 999 from other regulations ?
  - permit class actions to address scale issues ?
  - encourage bio-diversity ?
  - permit privacy invasive research & mitigation ?

Conclusions

- Lots of threats and they are evolving fast
  - clear proof that Darwin was right!
- Myriad possible causes
  - but most actors are doing their best and cannot be expected to solve it alone anyway
- There are ‘No Easy Solutions’
  - but can see some general principles on how to move forward plus a few specific tweaks

Personal Internet Security

Dr Richard Clayton

`http://www.cl.cam.ac.uk/~rnc1/`

UNIVERSITY OF
CAMBRIDGE
Computer Laboratory