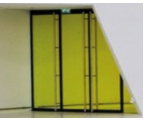
Measuring the ups and downs of cybercrime

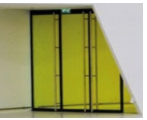
Dr Richard Clayton
University of Cambridge

UNIVERSITY OF CAMBRIDGE
Computer Laboratory



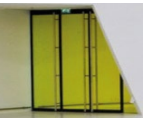
My background

- I’ve been looking at online abuse (spam, phishing, malware, DDoS etc) for 20+ years
- My approach is data driven (I count things)
- I have obtained many datasets from industry under NDAs and that has underpinned the work I have done (in collaboration with some very smart people)



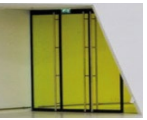
Our problem

- Everyone works in similar ways…
- We’re beginning to realise that no cybercrime papers in this field can be reproduced (data cannot be shared, results cannot be compared, conclusions cannot be validated)
- This does not really look like science…



Cambridge Cybercrime Centre

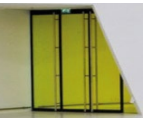
- I have 5 years funding from EPSRC
  - and some other money
- Currently 6 of us + PhD students & UTOs
  - Computer Science, Criminology & Psychology
- We collect & collate cybercrime datasets
  - and then do world class work on it



Data sharing

- AND we share this data with other academics
  - this is not “open data”, you have to sign paperwork
  - but we make data available at an early stage
    - (even realtime)
  - over 30 research groups now signed up

- I’ll share your data too if you like !
  - we already have appropriate legal agreements
  - “one stop shop” – we do due diligence & paperwork

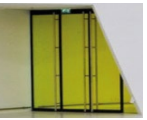


WEIS 2012

- "Measuring the Cost of Cybercrime"
  - leading academic authors
- Provide framework & measurement data
- Headline numbers:

tax fraud, VAT fraud, benefit fraud	$100s /person
fraud that was now online (banking &c)	$10s /person
"cybercrime"	10¢ /person

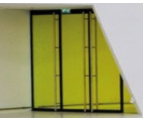
- BUT: spending ~$100 /person for defence costs



WEIS 2019

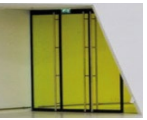
- Revised 2012 paper as “Measuring the Changing Cost of Cybercrime”
  - added three authors (and subtracted two)
- … & get pretty much the same result !

- BUT the differences and trends are very interesting …



Victim surveys

- Back in 2012 we thought that cybercrime was about half of all “property crime”
  - victim surveys show that we were right !
  - sadly, little consistency re questions or methodology
- Nevertheless, victim surveys much prized by criminologists because many crimes underreported, but care needed when scaling results to population levels…



Survey examples

US: 10% of population had an unauthorised debit

UK: 3.5m fraud offences/year – similar to theft

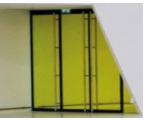
BE: >50% of businesses experiencing cybercrime

FR: 3m cybercrime events/year (4% population)

AU: survey => losses in the $100s/person/year

E-CRIME EU project: 6 countries

10Euro/person/year



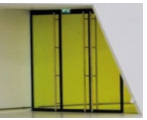
Since 2012…

CHANGES

- Android / iPhones replacing Windows (& Macs)
- services are moving to the cloud
- social networks pretty much ubiquitous
- Internet of Things (IoT … the S stands for security)

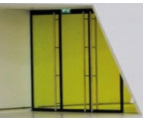
UNCHANGED

- law enforcement budgets
- the key role of technology firms



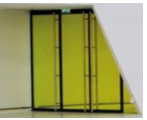
Payment fraud

- UK:
  - card-not-present fraud: 2 X in volume & value
  - e-commerce events rising, mail & telephone falling
  - lost/stolen card fraud 3 X volume but 2 X value
- BUT: payment volume has more than doubled
  - better analytics & chip-and-pin means we're winning!
- Same pattern can be seen in US & Europe



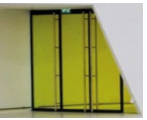
Business Email Compromise

- Multiple scams affecting businesses:
  - invoice replacements (send payment here)
  - CEO fraud (asking for wire transfers)
  - gift cards (“I want to give staff a surprise bonus”)
- Also affects individuals (especially real estate transactions)
  - termed “Authorised Push Payment” fraud in UK, and “Email Account Compromise” fraud in USA



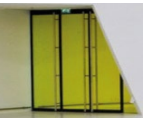
BEC statistics

- Internet Complaint Centre (IC3 == FBI) publishes stats
  - 2014 $226m 2 417 complaints
  - 2015 $246m 7 837 complaints
  - 2016 $361m 12 005 complaints
  - 2017 $676m 15 690 complaints
  - 2018 $1298m 20 373 complaints
- Worldwide now $12.5bn since 2013



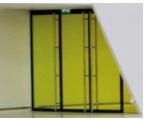
Ransomware

- This wasn’t in our 2012 paper (though by 2012 prepaid money cards were already being used by ransomware)
- Reliable figures show not a lot of money:
  - $16m criminal revenue 2015-17
- But of course actual losses are several orders of magnitude higher



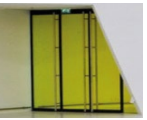
Cryptocrime

- Many other cryptocurrency enabled crimes
  - $7.1m ponzi scams; $52m mining scams; $36.3m fraudulent ICOs; $6m fraudulent cryptocoins; $5m fake cryptocurrency services
  - this SEC data undoubtedly underestimates the issue
    - BitConnect may have cost investors $1bn
- Exchanges lost $1bn to hackers in 2018
- Overall cost is in the $2bn/annum range!



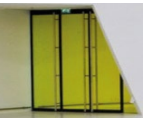
PABX fraud

- 2012 global cost of telecoms fraud was $40bn
  - mainly unpaid bills, $4.96bn was PABX fraud
- But phone calls (often VOIP) are now cheaper !
- So headline figure is now down to $29.2bn
  - and dropped 23% from 2016 to 2017
- PABX fraud now $3.88bn (was reselling service to expats, now calls to premium rate numbers)
  - “Yes, I will accept the charges for a call to Zaire”



Industrial espionage & extortion

- There is still no compelling evidence as to the level of losses but nevertheless this topic still talked up by Governments
- Also nothing to support wild claims about extortion losses
  - yes, DDoS extortion is a thing, but amounts are small

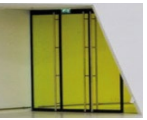


Wannacry & NotPetya

- Overall losses perhaps $1bn to $2bn
  - BUT caution! original TSMC (Taiwan chipmaker) losses of $255m later scaled back to $84m
- Mondelez is claiming $100m under their policy from Zurich Insurance for NotPetya losses
  - but this has been refused under an “act of war” clause (& simply because cyber not covered under “property & casualty”) The courts may settle this one
- Most state activity not linked to financial losses

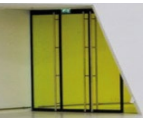
Summary of the current state

- Payment fraud is up, but transactions up more
- Cryptocurrencies enabling new scams (but the big money is being lost in schemes resembling traditional investment frauds)
- Structural change has reduced telecoms fraud
- Some crimes disappearing, others appearing
  - anti-virus fraud almost disappeared
  - tech support scams growing very rapidly



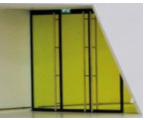
Plus ça change!

- The big money is still in tax fraud, VAT fraud, welfare fraud etc.
- Defence costs outweigh actual losses
- Criminals still don’t think they’ll be caught (and are mainly correct)
- Tech has changed markedly, but economics is much the same



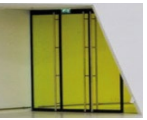
Booters (aka stressers)

- “Booters” are websites selling DDoS
- Low cost (10 Euro gets you a month of attacks)
- Mainly used by online games players
  - you can do better if you knock out the opposition “teamspeak” server & their two best players
- Some usage to attack schools etc
- Mainly use reflected amplified UDP DDoS

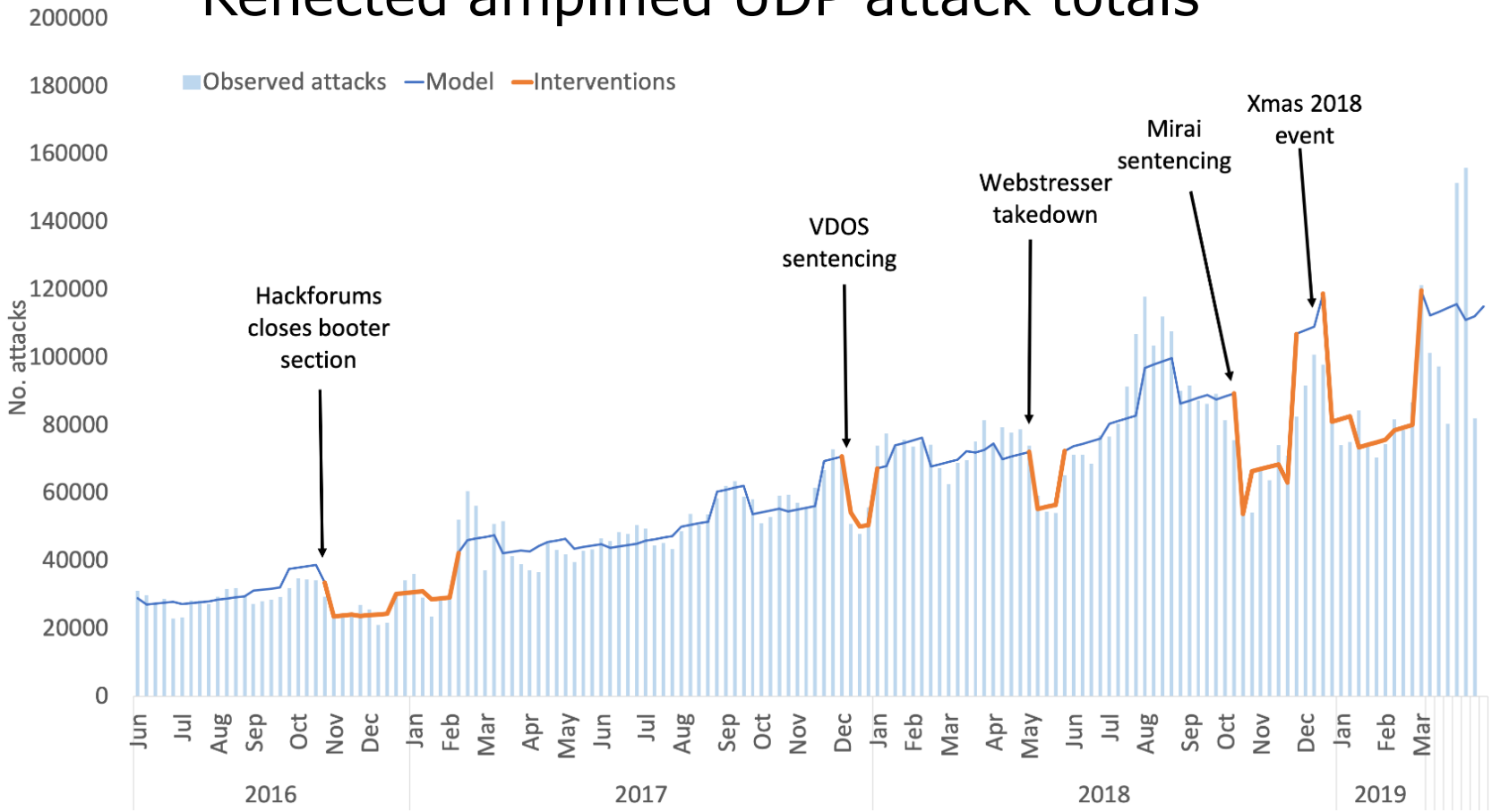


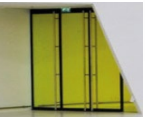
Reflected amplified UDP DDoS

- Many UDP services can send out lots of data in response to a single incoming packet
- Forging UDP source is used to create a DDoS
- We (CCC) run sensors to identify attacks
  - we pretend to be a reflector so we learn of victims
  - over five years of data available
- So we can count victims over time…

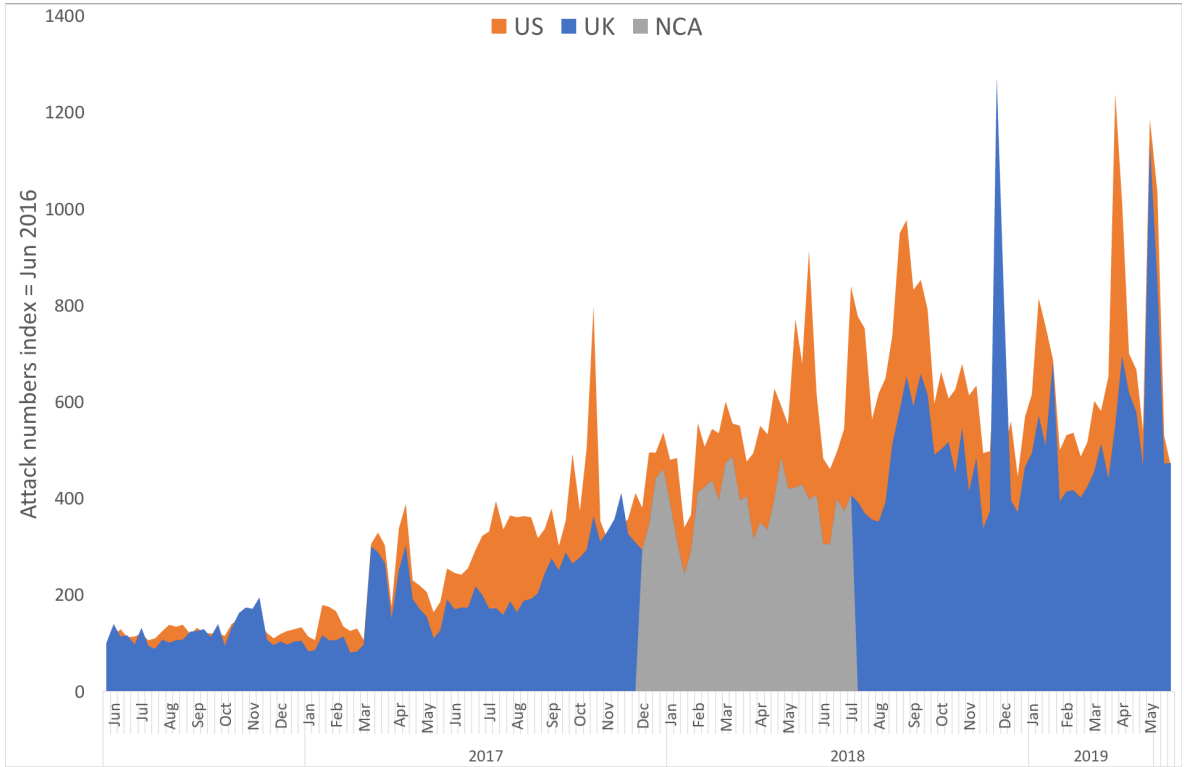


Reflected amplified UDP attack totals



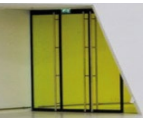


Effect of NCA advertising in the UK



NCA purchased Google search adverts for “booter”, “stresser” &c, the text said booting is illegal and the link led to an explanatory webpage

Adverts only served to UK IP addresses



Blog:

`https://www.lightbluetouchpaper.org`

Data:

`https://cambridgecybercrime.org`

Me:

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

UNIVERSITY OF CAMBRIDGE
Computer Laboratory