Trends in Sophisticated Hacking

Dr Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Berlin

14th December 2011

“Security Economics”

Security Group,

Computer Laboratory,

University of Cambridge

- Big focus on “security economics” the new (since about 2000) approach to the understanding of computer security
- Looks more at the “economics”; less at the “computer science”
- e.g. Who loses money if this security problem is not addressed (and therefore has an incentive to fix it) ? Who did the security design ? and who is now actually in a position to fix it ?

Trends in sophisticated hacking

I was given this title to talk to …

… but in practice I’m going to try and persuade you that almost all of the bad things aren’t especially sophisticated !

Malware

- Malware is general term for “malicious software”
  - never was very useful to distinguish virus / worm / trojan etc.
  - lots of history: Brain, LeHigh, Melissa, ILoveYou
  - first spread on floppy disks & then email
  - every copy was the same, and it was mostly harmless
- Malware today spread by many different vectors:
  - email (still! lots of examples stopped by your spam filter)
  - drive-by infection (on both good and bad websites)
  - over the network and via memory sticks (eg Stuxnet of course)
- Often every sample is different (so AV stats are meaningless)
  - “server side polymorphism” gives everyone a different copy
  - “if you see two samples the same, it’s a false positive”
- Harm is credential theft and botnet membership
  - for corporates, insiders and intruders matter more than malware

Understanding malware

- Impression still given of diligent AV analysts slaving into the small hours to tease out every detail of new attack
  - sample is merely run within virtual machine (VM) [in a huge farm]
- Very little malware is actually analysed
  - once it's detected/removable, AV company's job is done
- Very little malware is correctly categorised
  - names have no value to AV company, so no effort to make correct
- Much malware is yesterday's binary repacked
  - but, there is almost no tracking of when improvements occur
  - but, would be enlightening to know what changed since yesterday
- Behavioural analysis has significant limitations
  - stuxnet spreading via network printers was missed for some time
  - assumption is that malware will not spot it is in a VM!

Is AV relevant any more ?

- AV detection rates reported (Cyveillance) to start around 20%
  - surprising that is so high, when criminals test before shipping
- Mass-market malware just asks for permission to be installed
  - this entirely sidesteps operating system controls
  - much success with codecs to view Britney Spears video
  - some cheats for online games steal credentials
  - foto ☺ http://www.x-facebook.com/album.php?richard@yahoo.com
- Detection of commercial monitoring software is poor
  - many products sold for child/employee monitoring…
  - … also used by stalkers, ex-partners etc.
  - AV generally doesn't detect this – they'd have to purchase samples; and would end up embroiled in lawsuits
- What most people need is "desktop protection" not AV per se

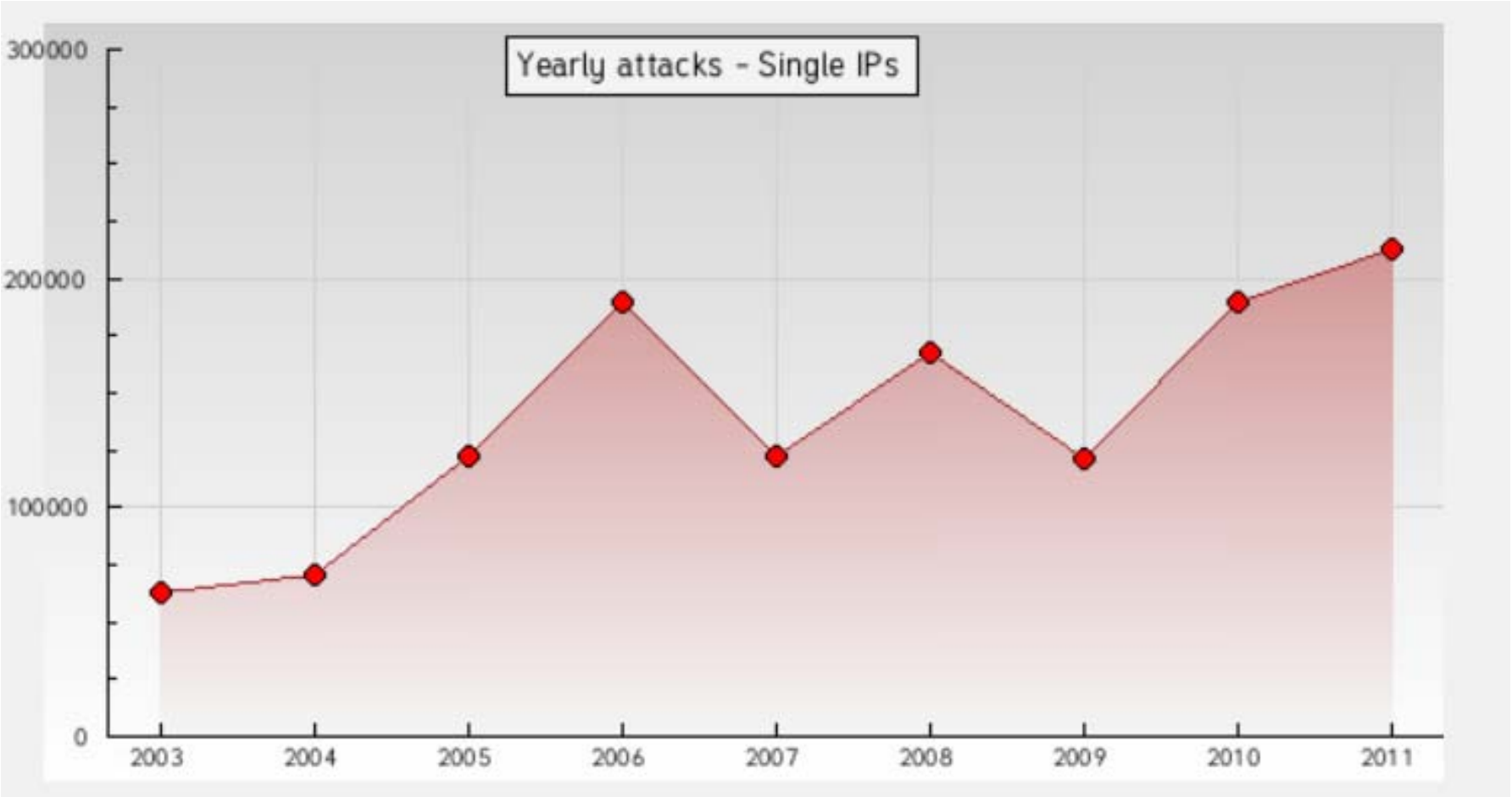
Was Stuxnet different ?

- Delivery mechanism: nothing especially remarkable
  - but clear that thought put into spreading mechanisms
  - did not contain lots of brand-new attacks
    - codebase likely to have been purchased (or stolen, or work for hire?)
  - some attention paid to obfuscation
  - seems to have been tested beforehand
- Payload was carefully designed
  - much attention paid to avoiding collateral damage
  - crypto certificates were stolen to order
  - tested beforehand
- Undoubtedly not the first professionally developed malware
  - the 2004 “Witty Worm” was very unusual as well
  - hallmark of malware from a “nation state” may be the availability of their own internet (small I) on which to test!

Hacking into machines

- Impression (now mainstream in Hollywood) of lone experts with poor social skills and extreme levels of technical ability
- “War Games” may be closer ? limited skill and some luck
- Underground Economy has led people to make their own luck
  - mass compromises of insecure WordPress installs
  - evil searches (no longer any need for “scanning”)
  - magelangcyber.web.id (9 months, 110K machines, 27 people > 1K)
- Payloads have been deskilled
  - PHP shells, PHP mailers, PHP scanner, PHP relays
  - phishing kits (many with backdoors)
  - Zeus, SpyEye etc. (malware with a support contract)
- 2011 notable for rise of the “hacktivist”
  - often SQL injections attacks (OWASP #1) to extract databases

Zone-H defacement data



Kevin Mitnick (a quick case study)

- Portrayed as an über-hacker; and was FBI Most Wanted (cyber)
- His main skillset was social engineering
  - RSA token story is illustrative
- Difficult to protect against people like Mitnick
  - requires your receptionists to be rude to everyone
  - requires you to refuse to assist random colleagues
  - requires you to distrust CLI to distinguish internal phonecalls
- This is now echoed in advice about preventing spear phishing
  - discard attachments from colleagues unless they ring you first
  - don’t put any details of staff on your webpages
  - don’t keep pages with links to internal resources
  - never mention your job when interacting in social media
  - of course, this is what intelligence operatives always did…

The “Myth of the Superuser”

- Paul Ohm, 2008
  - identifies “Superusers”, those with “power” that most don’t have
  - the “myth” is that online conflicts cannot be resolved without dealing with the Superusers
  - he gives lots of examples of stories about supposed Superusers which were exaggerations or apocryphal
  - argues that the myth is leading to unjustified loss of civil liberties
- There’s something very similar going on with “hacking”
  - often said that the APT attacker will always succeed
    - c.f. Stanley Baldwin 1932 “the bomber will always get through”
  - APT attackers seen as highly skilled deployers of 0-days
    - some disappointment when clicks are on perfectly ordinary malware
  - multi-stage attacks regarded with undue awe
    - #1 hack RSA, #2 hack Lockheed etc.
  - i.e. excitement about the A in APT (whereas P is what’s relevant)

Cyberwar/Cybersecurity and Cybercrime

- Cyberwar is being rebranded as Cybersecurity
  - rather as the “War Office” is now the “Ministry of Defence”
  - what we actually see is some cyber-espionage and some cyber-riots
    - events in Estonia and Georgia of limited technical interest
- Contrast with Cybercrime, which is all around us
  - but most attacks fairly low value, so hard to justify investigating
  - evidence is difficult to collect (the private firms that run the infrastructure have difficulty collaborating with agents of the State)
  - much crime is cross-border, so traditional policing struggles
- In the “Wild West” a key role was played by the Pinkertons
  - current ad hoc industry “trust groups” are making a real difference
  - so maybe we should abandon efforts to reform policing ?
  - but note their role in strike-breaking from 1870s onwards, so there’s a risk to a privatised Internet security approach

Conclusions

- "It's the economy stupid" (Carville, 1991)
  - but it's psychology that makes individuals do stupid things
- "Any sufficiently advanced technology looks like magic"
- Since we haven't yet created a compelling model for explaining security, we ply our trade using fireside "war stories"
  - and stories are much more fun if the people in them are clever and innovative and achieve surprising things that we didn't forsee
- This leads us to believe that concentrating on defeating advanced attacks will make us all secure
  - whereas the real damage is from boring run-of-the-mill stuff
  - especially when the attacks can be productionised …
    - but we're not even sure about that, because we are woefully short of wide-ranging, unbiased, reliable data (because collecting data is less fun than telling each other exciting stories as we huddle in the darkness)

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

http://www.lightbluetouchpaper.org

Dr Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Berlin

14th December 2011