A Very Deeply Cynical (But I Venture To Suggest Entirely Damning) Appraisal Of Every Possible Payment Scheme For Electronic Mail, Past, Present And Future

(Present Company IS included)

Richard Clayton

University of Cambridge

CEAS : 30 July 2004

A Quick Taxonomy

- Real money (dollars, pounds, dinars...)
  - who pays? who receives? who rakes it off?
- Processing time (Proof of Work, HashCash)
  - robust (if properly designed by crypto experts)
    - fragile if augmented with extras such as whitelists
- Human time (Capchas, HIPs)
  - is the puzzle bound to the problem? (free porn!)
    - however, in South India, going rate is $0.11/hour...

The Problems for Real Money

- People will regulate it
  - EU Directive on E-Money (2000/46/EC)
- People will walk away with 2.5% of it
  - there's a real cost in running a system + greed!
- People will steal it (in imaginative ways)
  - some systems rely on your friends not cashing cheques you write. Suppose an ISP sysadmin sometimes removes cheques before delivery?

Payment: What Do You Buy?

- Are you paying for guaranteed delivery?
- If there a refund for delivery failures?
- Can people read the message and then lie about delivery?
- Can an ISP lie about delivery?
- Can an ISP lie about sending?
  - if there is “real money” involved then why should people tell the truth about anything ?

Payment: Double Spending

- Many schemes send crypto tokens along with the email to show it is genuine (or to represent the money)
- If the spammers send bad tokens (or good tokens they are re-using) then how do we know? We cannot avoid checking every email token for validity and unique usage
  - looks like a big bandwidth / processing cost

Payment: Settlement

- ~1200 million (real) emails per day
- ~2000 million phone calls per day
  - but almost all are local to a single telco
- However less than 500 telcos worldwide
  - many more ISPs to dispute with each other
  - and a very different underlying trust model
  - now imagine the main token provider going bust (or into ISP Z's ownership)

Who Pays for Security Flaws?

- If my system is compromised (>2 million systems are) then do I have to pay for the 30,000 emails sent before anyone notices?
  - if not, who does pay?
  - or are we joking that this is a payment scheme?
  - or am I barred from writing my user-base about a new security bug-fixing release? (I would need a bank loan to cover the cash-flow!)

How Much Payment?

- At 30 responses per million then 1/10th of a cent per email means you need to be clearing $33/sale to make spamming viable
  - If 1/20th of a cent (Indian Capchas) it is $16
  - BUT at a 0.7% response rate then a $33 profit means you can spend 23 cents per email
- For “proof-of-work” then reckon on a PC costing ~$1/day so that 1/10th cent charge maps into about 86 seconds of processing

Proof of Work: Steal Cycles

- Easy to steal a million machines
  - about 2 million have insecure proxies
  - large virus infection often infects a million
- With these machines you can fill 1% of the world's mailbox, even if we restrict every machine to just 10 emails/hour
- Stealing is fatal blow for "proof-of-work"
  - infected hosts are hard to detect !

The Introduction Problem

- Many schemes whitelist “friends” (because the scaling breaks very quickly if you check everything every time)
- Who is a friend? my bank outsources email !
- If I recognise friends (or bankers) using certificates, then we need a global PKI (a decade later, we now know to be impossible) OR I run my own (which just restates the problem)

An Introduced Spammer

- Spammers currently send the same spam to lots of different people
- What if spammers pretended to be friends?
  - jumping through all the hoops I set out
- Then rapidly send lots of different spam
  - until I cut them off, but that's too late!
  - viz: why assume that they will continue to only advertise their own products?

What is Payment For?

- To stop spam for low-margin products?
  - spammers will evade the system, they will steal the money and MODIFY WHAT THEY DO
- To make email ads work for the DMA?
  - “permission based” is the only viable long term approach, so why would they want payment?
- To take some money out of my pocket?
  - and put it into someone else’s!

Summary

- Capchas will be solved in Madras suburbs
- Proof-of-work will be computed on virus-infected machines in our kids' bedrooms
- Real money will be stolen (or sliced away in handling fees and conversion charges)
- And the spammers will pretend to be your friends for just long enough……

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