Limits of Security Technology: Lessons from the Spam Wars

John R. Levine
Taughannock Networks
New York USA
Turn the clock back to 1996 ...

• We start to see spam
• Wow, how annoying
• No problem, we’re technical experts
  – And we’re sure it’s a technical problem
  – So …
We invent filters
But spammers react
Why don’t filters work?

• Differences between spam and good mail
  – Spam is badly spooled
  – Uses words rarely found in good mail
  – Sent in vast quantities
Why don’t filters work?

- Spam is badly spelled
- Uses words rarely found in good mail
- Sent in vast quantities

- Spammers can use spell checkers, too
- Spell it v1@gra and use HTML tricks
- Randomize spam so it all looks different
Why don’t filters work?

- Spammers can use spell checkers, too
- Spell it v1@gra and use HTML tricks
- Randomize spam so it all looks different
- Sending mail only gets cheaper
- Looks increasingly like legit bulk mail
- Your bank mentions mortgages
- Miscategorize all bulk as spam
- Follows technology curve
Filtering today

- Ever more aggressive filters …
- … ever more lost mail
- Pity the IT department
  - Delivered spam: immediate complaints
  - Lost mail: eventual complaints, maybe
Filtering today

- Ever more aggressive filters …
- … ever more lost mail
- Pity the IT department
  - Delivered spam: immediate complaints
  - Lost mail: eventual complaints, maybe
Filtering today

- Unwinnable arms race
  - Users tolerate more and more lost mail
  - Which isn’t good for anyone
- Some new work
  - Communities of senders
  - Of who?
Kick the Spammers Out!!

• Spam is against the rules
• And increasingly against the law
• So why are they still connected?
Kick the Spammers Out?

• Some ISPs kick harder than others
• It’s really easy to hide
How do spammers hide?

- Countries with weak laws
- ISPs with weak policies and AUPs
- Route mail through insecure third parties
  - All 500,000,000 of them
- Lie about who you are
  - Technical spoofing
  - Fake affiliate, fake networks, fake everything
Who’s sending that mail?

- Internet resilient against external threats
  - Not internal threats
- No internal security
  - Except against technical problems
- You can be whoever you want
Who’s sending that mail?

• You can be whoever you want
  – Which is fine
  – Except when it’s not
• Spoofing to hide from filters and ISPs
• Spoofing to defeat whitelists
Verification and Authentication

- Verify source of message (SPF, Sender-ID)
- Digital message signature (DomainKeys)
- All to detect and deter forgery …
  - … which is a problem, but it’s not “spam”
- Add confidence that sender is genuine
  - … but spammers have identities, too
Certification and Reputation

• Yes, it’s definitely from xuxle.net
• But who’s that?
  – Just a cyber identity?
  – Tied to meatspace ID?
• Do we want their mail?
Certification and Reputation

• Certification
  – Senders pay for recommendation
    *TrustE, BBB Online, Habeas, Bonded Sender, …*
  – Mostly about delivering good mail

• Reputation
  – Users buy reports, like a credit bureau
    *Spamhaus, MAPS/Kelkea, …*
Certification and Reputation

- Not very technical
- At best can hide spam, not stop it
How soon will these happen?

• Is a half fix better than no fix?
  – Not if it precludes a good fix
  – Not if it breaks things that work now

• Technical changes are slow
  – For good reasons
  – Not just technical “purity”
Who authenticates?

- Authenticated identities are valuable
- Lacking one, you are at a disadvantage
- What if you can’t afford to buy one?
- What if authorities say you can’t have one?
Not so technical futures

• **Best Practices**
  – Emerging trade groups set standards

• **Litigation**
  – Verification and Authentication help build cases

• **Legislation**
  – CAN SPAM didn’t work in the U.S.
  – Want to try again?
Where does technology fit in?

• Very hard to secure an insecure system
  – So design it with security in mind
• Technology: morally and politically neutral
• We need to decide what we want
  – Anonymous speech?
  – Virtual or physical identity?
  – Closed vs. open systems?
Limits of Security Technology: Lessons from the Spam Wars

John R. Levine
Taughannock Networks
New York USA