TEU00311

What is the Internet doing to me? (witidtm)

Stephen Farrell
stephen.farrell@cs.tcd.ie

https://github.com/sftcd/witidtm
https://down.dsg.cs.tcd.ie/witidtm

Good news on Assignments

- You have/had 4 assignments from me
  - For 60 marks total
- You have/will-have 1 from Dave
  - For 80 marks total
- Those will be all!
  - We'll multiply by 1.25 to get to 100%
- Note: **Do the assignments** – I predict that anyone who's made a reasonable attempt at all assignments won't fail! (It would be an achievement to fail in that case;-)
- Reminder: **Anyone who hasn't done enough assignments will need to do a supplemental exam!**

Today’s Practical

- 4 “tables” - idea is to rotate amongst ‘em
  - Build/configure an OpenWRT home router
  - Install and play with Ubuntu
  - Setup a web server
  - Play with brower plug-ins and open-source alternatives
- Nov 27th session will be a repeat and/or build on what you did 1st time
- We’ll be in the LCR, from 1400-1800
- Note: I’ll be getting the kit ready between now and then, so things may still change, if stuff doesn’t work:-)

Additional Practicals

- Given good news on assignments, these are now just for fun
- Who’s coming today?
  - At 1400? Later?
- Who’s planning to come on Nov 27th?
- If you can’t make either, but have questions or want to chat, I’m available, just mail me

Lots about eMail

- Thursday (remote) guest: Janet Jones, Microsoft (with help from Sean Stevenson)
- With more than 20 years of experience, Mrs. Jones has an extensive background in technology, security and messaging. She led deployments and supported Microsoft's first worldwide cloud messaging implementations and currently works in Microsoft's Customer Security and Trust Engineering organization as a senior security program manager driving initiatives for their Secure Development Lifecycle and Operational Security Assurance programs. Mrs. Jones also participates in several other industry organization's initiatives that work toward securing messaging and data privacy. She is vice-chair of the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG – https://m3aawg.org).

To tee that up...

- Basics of Internet mail architecture
- Spam
- email security and privacy tools

- Will mention in passing: Phishing, malware distribution

Mail pre-history

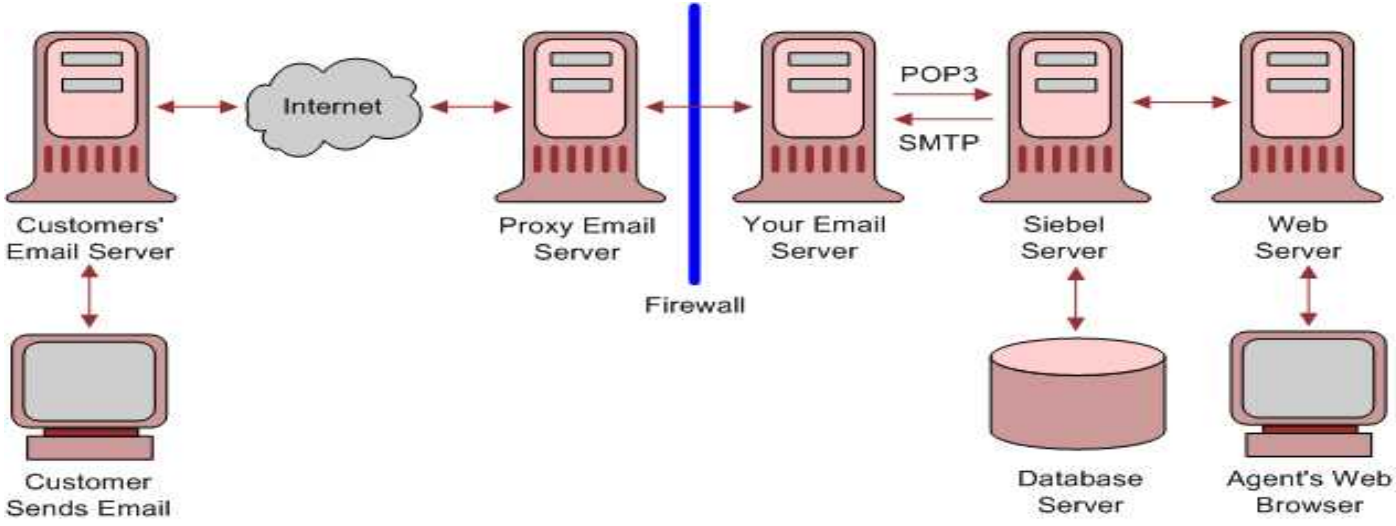
- There used to be non-Internet email systems
  - uucp, X.400, other proprietary
- Internet email “won” - largely because it could connect all the others
- Fundamental basis of email is that anyone can (try) send mail to anyone, without needing permission first
  - Prime requirement: deliver the message, at all costs!
    - there really is no marginal cost:-)
  - That allows mail to be the basis for most other Internet/web services (e.g. so you can sign-up or do a password reset)
  - That also allows spam and other nasties

Mail as it is...

- Mail address: user@domain
  - “user” is left-hand-side (LHS)
  - “domain” is almost always a DNS domain
    - That’s basically how mail gets routed to recipients
- LHS is (or should) only interpreted at the recipient’s server(s)

Email Architecture

- See RFC5598



https://docs.oracle.com/cd/E63029_01/books/SecurHarden/img/architecture_email_v.gif

Drive-by Terminology

- MUA, MTA, MSA, MDA, MS …
- Message envelope
- Forwarder, exploder, …
- Message headers:
  - From:, Sender:, Resent-From:
- 2821/2822
  - EHLO/HELO

Moar Terminogy

- Protocol for fetching messages from MS to MUA: IMAP
  - Internet Message Access Protocol
  - Earlier similar thing: Post office Protocol (POP)
- Protocol for sending messages from MUA to MTA, or between MTAs: SMTP
  - Simple Mail Transfer Protocol
- Today: all of those should really be run over TLS
- If not, you’re using the wrong service!

Spam

- A “first principles” approach

https://www.theguardian.com/environment/2017/feb/13/extraordinary-levels-of-toxic-pollution-found-in-10km-deep-mariana-trench#img-1

What is spam?

- Various acronyms:
  - Unsolicited bulk email (UBE)
  - Unsolicited commercial email (UCE)
- Spam is bad:
  - Resource consumption
    - Filters, scanners etc. cost time & money
  - Malware
  - Phishing attempts

Sometimes hard to know…

HILARY TERM GREETINGS FROM THE COLLEGE CHAPLAINS The College Chaplains send best wishes to all, and would like to bring the following upcoming events to your attention. They are open to any students or staff members who wish to join us. …

Original spam tricks

- Just send email!
  - Ahh…the naivety of it all!
- Email to list
  - Listservers got better, e.g. subscriber only with controlled subscription
- Forge headers
- Send via open relay
  - Used to be a lot of these, very few now
    - toad.com is an exception!

More spam tricks…

- Confusion:
  - accounts@paypa1.com
  - support@eboy.com
  - postmaster@boi-support.com
  - About to get worse thanks to I18N
  - security@bigbank.com
    ^ Unicode 0430 is cryllic small ‘a’
- Throwaway domains/addresses
- Zombie hosts
- Trojans
- Fake ISPs

Yet more

- HTML messing
  - Colour-related
  - Relay sites
  - Encoded URIs
  - Font size 0: break words with zero width spaces

How much spam is there?

- Lots
  - Hard to get good figures, these are ones I’ve overheard
- ISP backbones:
  - 70% + of email traffic
- Delivered mail:
  - 40% + delivered
- Increasing or not?
  - Harder to tell if MTAs silently filter

Some Anti-spam techniques

- Content filtering (Bayesian, etc.)
- DNS Black Lists (SORBS, DNSBL)
- Register of known spam operators (ROKSO)
- Greylisting
- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain Message Authentication Reporting and Conformance (DMARC)

End-to-end (e2e) email security

- That’s where you use cryptography to protect messages between the sender and recipient
  - Rather than just between each “hop” on the path the mail follows
- There are two different standards for how to do that: S/MIME and PGP
  - S/MIME is mostly used inside enterprises/govt
  - PGP is mostly used by nerds or smallish groups
- Since you can choose PGP and would only likely have S/MIME forced on you, we’ll look a bit at PGP

Pretty Good Privacy (PGP)

- PGP can do all that S/MIME does
- PGPMime is RFC 3156
- PGP’s basic formats in RFC 4880
  - Not ASN.1 based (TLVs)
- Web-of-trust model != X.509 PKI
  - But you don’t have to
- Most important use-case: package signing

PGP Key Management

- X.509-based PKIs are hierarchies
- PGP WoT based on user's signing one another's keys, with possibly many signatures per public key
- PGP Key IDs are hashes
- PGP key servers exist
- Usability: sucks:-(
- Details: lots of HOWTOs on the web

S/MIME and PGP Deployment

- Most MUAs suport s/mime or PGP either built-in or as an option
  - There are also “plug-in” products
- And mostly then *can* work together
  - I’ve used both, PGP more usable (via Thunderbird/Enigmail)
- But secure mail is not ubiquitous
  - Why?

e2e email security barriers

- Designs pre-date web user agent which changes trust model (where's the private key kept? Needs new infrastructure)
- Needs all major email service providers (yahoo, hotmail, gmail) to deploy the same thing which also needs to be implemented by all major user agent developers (microsoft, mozilla, apple, google)
- Public key retrieval needs to be fixed (doable if the above done, but a killer if not done), likely with some new PKI (doable but who's gonna pay?)
- Mail headers need to be protected as users don't get that S/MIME and PGP only protect body and not e.g. Subject, From (new enveloping protocol needed, can be done but kludgy)
- We need to unify S/MIME and PGP or pick one or we'll lose interop (it's ok if the other soldiers on for some niches)
- Users don't care much, so it has to be entirely transparent for them (needs significant UI work, co-ordinated across MUAs and significant web-UAs)

What can you do?

- Don’t react immediately
- Take **much** longer to write mails than to read mails
  - Always re-read before you send
- Don’t render mails as HTML if your MUA allows that
  - It’s ok to wait until you’re using a laptop to process mail
- Don’t assume any names/links displayed to you are real
- Treat all mails and and especially attachments with caution