Internet Junk

Quintin Russ

OWASP New Zealand Day 2012

31st August 2012

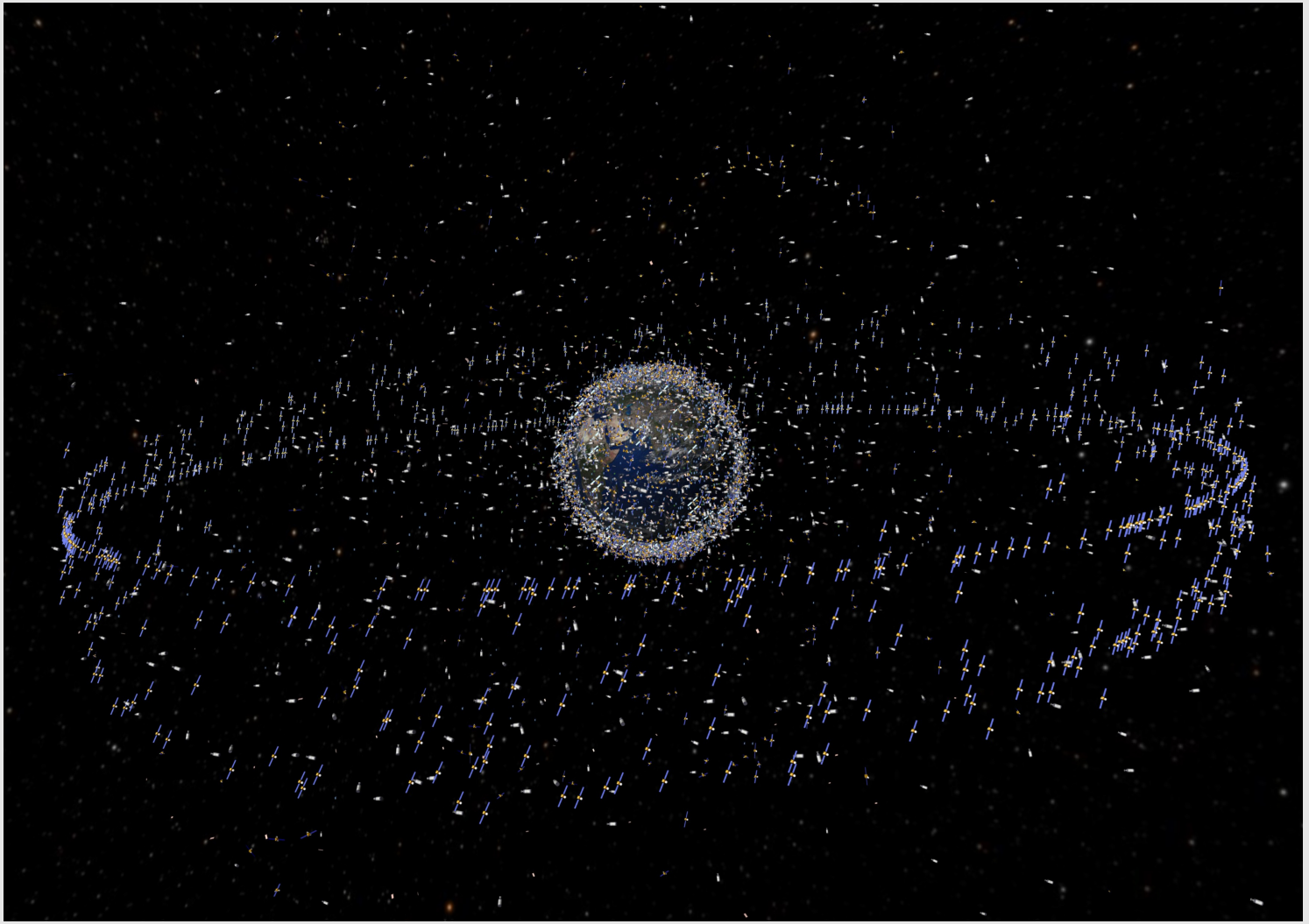
About Me

- Quintin Russ
  - Technical Director, SiteHost
    - Enjoys playing with Clouds
    - http://www.sitehost.co.nz
    - quintin@sitehost.co.nz
  - Web Developer in previous life
  - Focused on hosting infrastructure for last 5 years

Internet Junk

- Focusing on domain related issues today
- Ideas can be applied elsewhere there is trust
  - IP Addresses
  - Phone Numbers
  - Etc
- What exactly is Internet Junk?

Space Junk



Space Junk

"Space Junk is the collection of objects in orbit around Earth that were created by humans but no longer serve any useful purpose" – Wikipedia

Internet Junk

Space Junk

"Internet Junk is a collection of items which exist on the internet that were created by humans but have not or can not be deleted"

Internet Junk

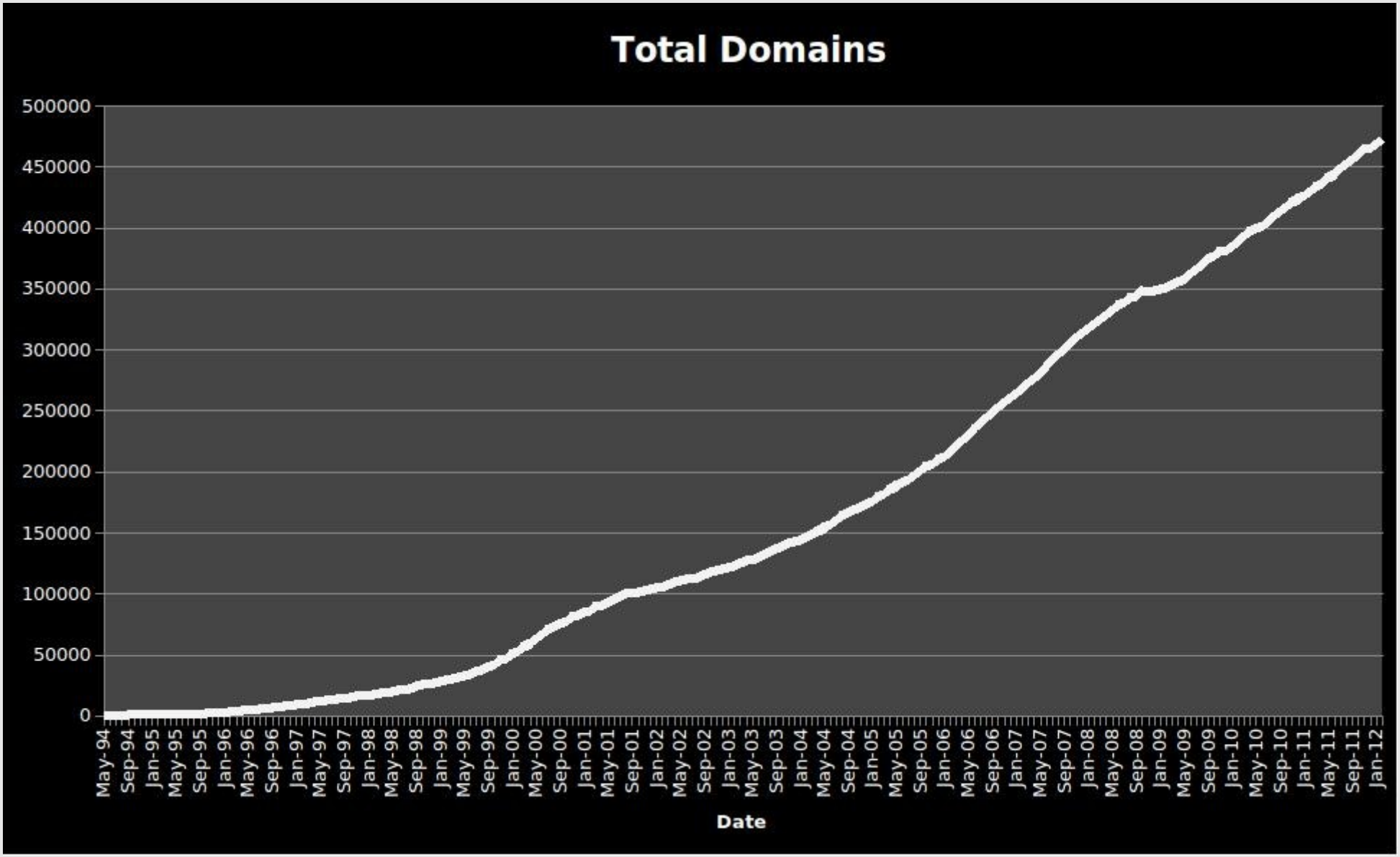
- In 2005 I registered a domain name
  - Very quickly began receiving emails
  - Some automated but a number which were not
  - These carried on for *years*
  - One email from a stranger even invited me over for dinner...

Internet Junk

Internet History

- First commercial ISP “The World” started 1989
- Actrix New Zealand's first ISP started 1989
- Commercialisation happened in 1995
  - SSL introduced by Netscape
  - Amazon, Ebay & Craigslist launched
  - IPv6 first proposed

Internet History



Internet Junk

Internet Junk

- Applications don't factor in domain lifecycle
  - Some don't even let you delete your data
- Domain system clearly says domains expire
- What does this do to the app security model?
  - It creates cracks between these systems
- Security is the art of finding cracks in processes
- Enough talk, show me what you mean already!

Internet Junk

- You own owasp.co.nz & use bob@owasp.co.nz
  - You use this email for all your accounts online
  - You let this domain name expire
- I come along and register owasp.co.nz
  - I setup a catchall inbox
    - Your accounts are now emailing me
  - I setup a wildcard A record
    - Your web traffic is now also coming to me
  - So what did I learn???

Internet Junk

Internet Junk

- What I learnt
  - There was a lot of Junk & Spam!
  - Average 1 legitimate email per day per domain
  - No providers unsubscribing released domains
  - Business case of purchasing domains for fraud
    - Domain Squatters could easily “lease” mail access out
  - Problem is getting worse

Internet Junk

- Its not just a couple of sites
  - Your credit card company
  - Your phone company
  - Your tax refund site
  - Your accounting software
  - Your online bookstore
  - Your favourite cloud provider
  - Your domain registrar
- I received emails from all of the above

Internet Junk

- Its not just newsletters
  - Online Purchases / Invoices
  - Password Reset requests
  - Business Proposals
  - System Bulk Processing
  - Backup Reports
  - An order for 10 tonne of liquid sugar?
- I received emails about all of the above

Internet Junk

- Example #1
  - Trademe.co.nz
  - Password reset requires:
    - Working Email Address
  - Password reset gives access to:
    - Your Name
    - Physical Address
    - Phone Number
    - Last 4 digits of your credit card

Internet Junk

- Example #2
  - Paypal.com
  - Password reset requires:
    - Working Email Address
    - Last 4 digits of your credit card
  - Password reset Provides:
    - Money

Internet Junk

- Just ask Mat Honan
  - Journalist who wrote article about his “epic hacking”
  - Entire digital life was destroyed in less than 1 hour
  - 4 Different accounts compromised
    - Amazon
    - Apple
    - Google
    - Twitter
  - iPhone, iPad, Macbook all remote wiped :(
  - http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/

Space Junk

"The very four digits that Amazon considers unimportant enough to display in the clear on the Web are precisely the same ones that Apple considers secure enough to perform identity verification" – Mat Honan

Internet Junk

- Why does this matter
  - Our ability to verify the chain of trust is critical
  - Users are storing more information online
  - This makes you or your application a target
    - Either directly or indirectly

Internet Junk

- Not just an issue for email
- Web requests
  - Web spiders
  - Legitimate Links
  - Restful / SOAP Web services
- And many more...

Thank you for listening, questions?

Internet Junk

Quintin Russ
quintin@sitehost.co.nz