Problematic of a Safer and more Robust Internet

AfNOG V

M. Alain Patrick AINA aalain@trstech.net

May 2004



What is the Internet ?(1)

A Network of Networks which share a common set of protocols

A place where many live, work and play.

A critical resource for many business that depend on E-commerce

A network always under pressures

- More users, devices connected and traffic



What is the Internet? (2)

A network theoretically impossible to map

- Or count its users
- Or list vulnerable hosts (or fix them).
- Or keep track of bad actors (or arrest them)

The Internet has become a new ecosystem

- Like biology: can be studied but not understood

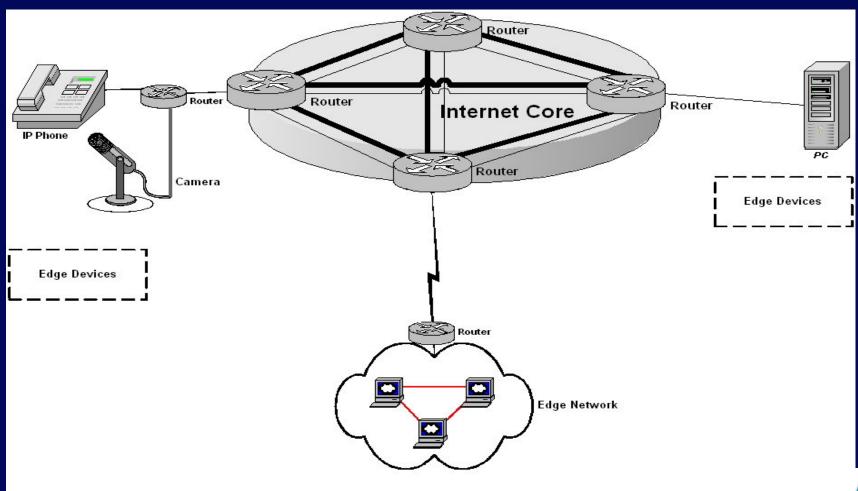


Consequence

The Internet must become and remain safer and more robust



How is it operated?





How is it operated?

The core is built by non-experts ISP

- Very little off the shelf technology or training
- Vendor defaults completely inappropriate
 Thus: no admission control on customer traffic

The edge is held by Host operators nonexpert technologists

- The Internet is full of dangerous places/people
- PC and DSL market allows universal access
 Thus: wide scale vulnerability and abuse



Example of past challenges(1)

Internet HOST.txt file

- Listed every internet-connected host of the day
- Impossible to update, maintain and scale

Solution: DNS

Classeful Internet addressing

- 100 "A",15000 "B",2000000 "C" networks
- Impossible to create and maintain routing table
- Foreseeable lack of IP address

Solution: CIDR



Example of past challenges(2)

DNS allow only 13 root servers

- Consequence of early IPv4 design choices
- Host population demands vastly better coverage
- Vulnerability to DDOS

Solution: Anycast

billion hosts allowed in IPv4

- Not enough for each person
- Not enough for each cell phone

Solution: IPv6



Example of past challenges(3)

The Internet doubled in size every 16 months from 1990 to 1999

- More users, devices, applications

Solution: Faster links (from 56K to up to 2.5G)

.com explodes

- Impossible to obtain short name
- More domain names business

Solution: new gTLDs



Necessary Next steps(1)

Make Infrastructure stronger, more robust Increase Interconnexion between ISPs

- Stop depending on few/large intermediaries
- Every metro needs its own IP exchange

Increase technology training

- Students in school
- Vendor engineers
- ISP operators and home users



Necessary Next steps(2)

Add security to the core Internet protocols

- Layers 3 and 4
- Routing

http://www.ietf.org/internet-drafts/draft-ietf-rpsec- routing-threats-06.txt

- DNS: was never secure, but must be

http://www.ietf.org/internet-drafts/draft-ietf-dnsext-dns-threats-07.txt

Make "mirror" copies of important servers

root and TLDs



Necessary Next steps(3)

Secure the edge

- Filter customer's traffic (RFC 2827)
- Better software engineering
- Wider used of updated software
- Control access to devices (routers)
- Use of security protocols and tools (patches, strong authentication, antivirus, S/MIME,PGP, SSL/TLS,SSH,IPsec, firewall...)



Can this be achieved? (1)

Changes to the Core is complex

- Required the coordinated actions of many providers and users
- Takes long time for the IETF community to obtain consensus and tune protocols
 - DNSSEC design started in 11/1993
 - Many things done
 - Many things to be done



Can these be achieved ?(2)

- Root key distribution and authentication
- Signing root zone
- Policies for crossing both non signed and signed zones etc..
 - Performance and scalability test

"An idea can work well in laboratory and testing, but fail in public broadband"

Must follow the robustness principle

- Be conservative in what you do, be liberal in what you accept from others"

Technologies Reséaux &solutions

Can these be achieved ?(3)

Different level of development

- Faster links in us, eu, jp etc...
- Slow and long latency links in many developing areas

More expensive routers needed Regulations restrictions etc...



Can these be achieved ?(4)

Innovation at the edge and end-to-end security

- is recommended(rfc 1958 and 3439)
- All designs must scale readily to very many nodes per site and to many millions of sites.
- Principles that seemed inviolable a few years ago are deprecated today.
- Principles that seem sacred today will be deprecated tomorrow.

TRS

Can these be achieved ?(5)

All of this will cost more money

- -Increase size and training level at ISPs
- -Increase training available to home users
- -Increase interconnectivity between ISPs

Internet usage fees will probably increase

New challenges will probably show up

- Normal life cycle of things



Some good news

Many Network Operators groups (NOG)

- Provide forum for the exchange of information among ISPs about problems and solutions

Many Emergency Response Teams

- Disseminate infos about vulnerabilities

Fast Fibers link reaches some other parts of the world

Many governments is getting involved in Internet's development and governance

Technologies Reséaux &solutions

Other tracks of reflexion

When can it be achieved?

- by 2009 ? 2014 ?

Is the current management and engineering systems of the Internet (ICANN/IANA, IETF...) efficient ?

- Many complaints about ICANN/IANA procedures
- Many complaints about IETF's mechanisms
 - Problems identified in www.ietf.org/rfc/rfc3774.txt



Conclusions

Biggest Internet engineering problem

- Scaling Internet Vulnerability is a problem for society
- Safety is more important than money and fun All must be taken seriously
 - African's operators must assume their part of responsibility

