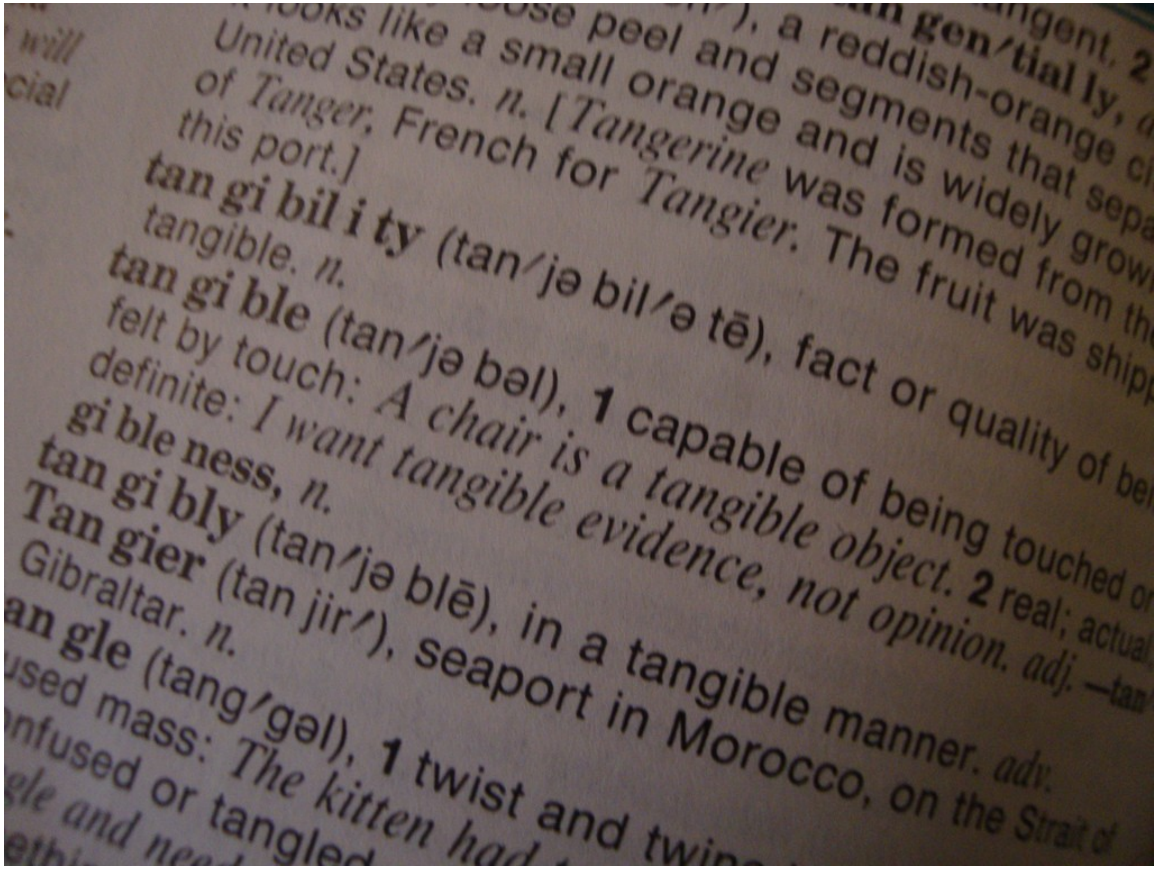
The Rapid Rise of the Mobile Multihomed Host,

and what it might mean to the network

Mark Smith
markzzzsmith@yahoo.com.au

AusNOG - September 2013

Mobile Multihomed Host – A Definition



will
cial

...n′), a reddish-orange ci... **tan gen′tial ly**, a... ...angent. **2**
...oose peel and segments that sepa...
...ooks like a small orange and is widely grow...
United States. *n.* [*Tangerine* was formed from th...
of *Tanger,* French for *Tangier.* The fruit was shipp...
this port.]

tan gi bil i ty (tan′jə bil′ə tē), fact or quality of bei...
tangible. *n.*

tan gi ble (tan′jə bəl), **1** capable of being touched or
felt by touch: *A chair is a tangible object.* **2** real; actual;
definite: *I want tangible evidence, not opinion. adj.* —tan
gi ble ness, *n.*

tan gi bly (tan′jə blē), in a tangible manner. *adv.*

Tan gier (tan jir′), seaport in Morocco, on the Strait of
Gibraltar. *n.*

...an gle (tang′gəl), **1** twist and twin...
...used mass: *The kitten had...*
...nfused or tangled...
...*gle and nee*...

CC Image courtesy of Julie Jordan Scott
http://www.flickr.com/photos/juliejordanscott/4247673227/sizes/l/in/photostream/

Mobile - moves around

Multihomed – connected to multiple networks, but not a router

Host – Hosts applications that use the network

MMHH - Smartphone

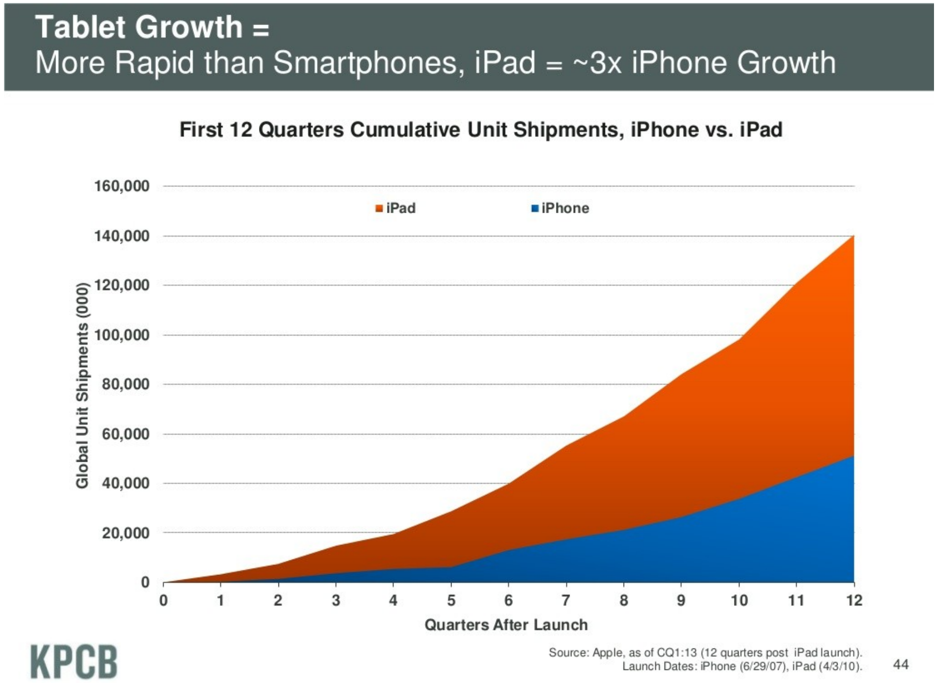
CC Image courtesy of Kārlis Dambrāns a.k.a. Janitors
http://www.flickr.com/photos/janitors/8781826986/sizes/c/in/photostream/

MMHH - Tablet

CC Image courtesy of Josué Goge
http://tinyurl.com/lr9ng9v

Rapidly Adopted

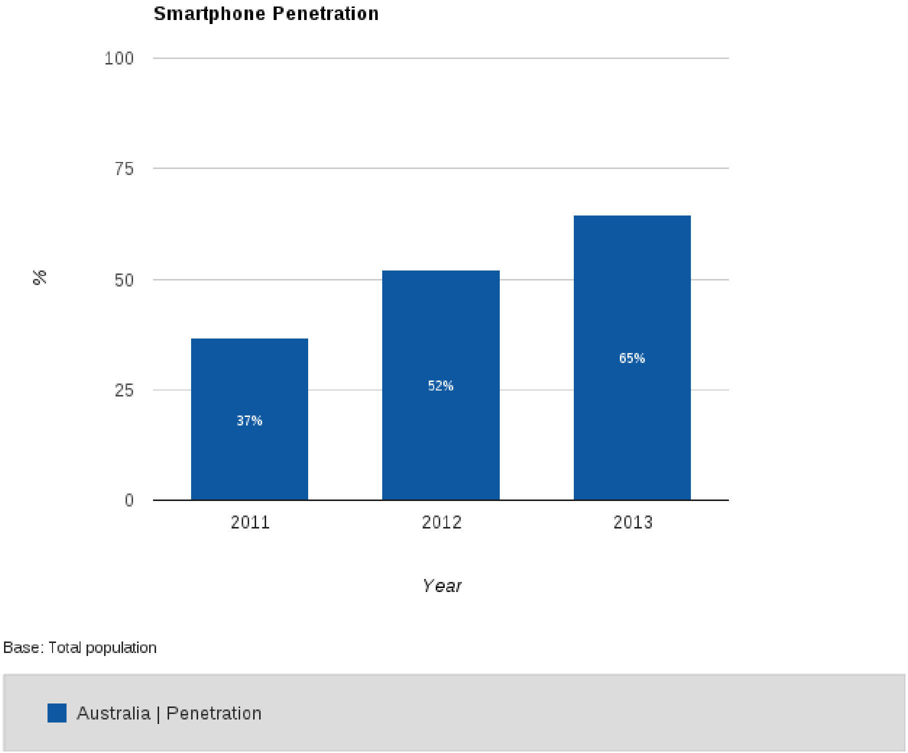
CC Image courtesy of Mr Thinktank
http://www.flickr.com/photos/tahini/6966762102/sizes/l/in/photostream/



Tablet Growth =
More Rapid than Smartphones, iPad = ~3x iPhone Growth

First 12 Quarters Cumulative Unit Shipments, iPhone vs. iPad

Source: Apple, as of CQ1:13 (12 quarters post iPad launch).
Launch Dates: iPhone (6/29/07), iPad (4/3/10).



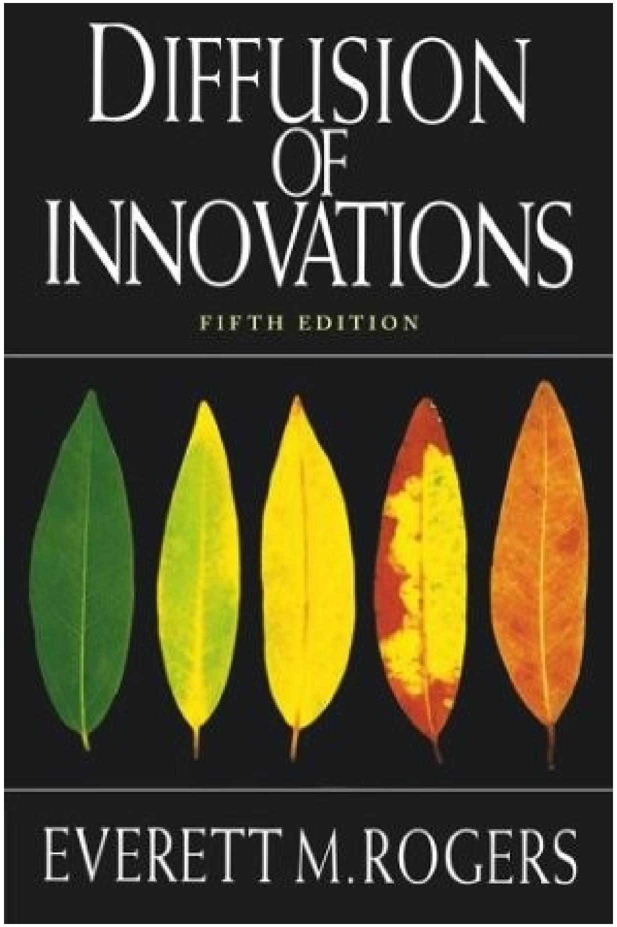
Smartphone Penetration

Base: Total population

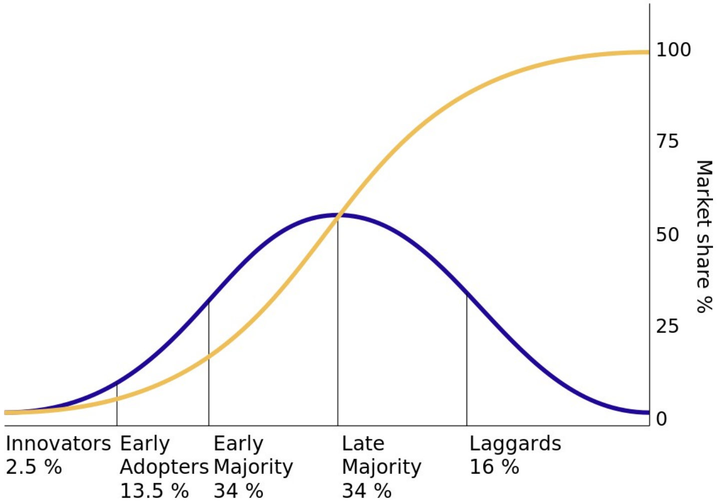
Courtesy “2013 Internet Trends”, KPCB, http://www.kpcb.com/insights/2013-internet-trends

Courtesy “Our Mobile Planet” http://www.thinkwithgoogle.com/mobileplanet/en/

Diffusion of Innovations



http://en.wikipedia.org/wiki/Diffusion_of_innovations



“An *innovation* is an idea, practice, or object that is perceived as new by an individual or other unit of adoption”.

5 innovation attributes that influence adoption

***Relative Advantage* -** Better than what you've had in the past

Smartphone/Tablet - Mobile rather than fixed Internet

***Compatibility* -** Similar to what you already know

Smartphone/Tablet - Pretty familiar GUI, finger instead of mouse

Complexity - Easy to understand?

Smartphone/Tablet - Intuitive to use, no manual required

***Trialability* -** Easy to “try before you buy”?

Smartphone/Tablet - Borrow a friend's, try in a shop

Observability - Easy to see others using it?

Smartphone/Tablet - People using them in the street, on public transport

A Bit of Internet Architecture

CC Image courtesy of azhararchitecture
http://tinyurl.com/n7whzjk

END-TO-END ARGUMENTS IN SYSTEM DESIGN
J.H. Salzer, D.P. Reed and D.D. Clark

When it comes to deciding where a function should be located and performed within a system,

“**The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system.** Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)”

So what is this really saying?

Applications exist on hosts (the **endpoints**), so functions related to how applications use the network are best done on the hosts

Example : TCP implemented on hosts, **not in the network**

Or Simpler

Do things where the results matter the most

Do things where the best knowledge of what is and isn't required is available

Sounds familiar ....

If you want something done properly, you need to do it yourself

http://en.wikipedia.org/wiki/Charles-Guillaume_
%C3%89tienne

Actually, Charles-Guillaume Étienne originally said “On n'est jamais servi si bien que par soi-même.”, which literally translates to,

"One is never served so well as by oneself."

So if the hosts are going to do it themselves to do it properly, **the network may as well be as simple as possible**,

and just carry the packets

CC Image courtesy of OliBac
http://www.flickr.com/photos/olibac/2415284302/sizes/l/in/photostream/

Dumb Network, *Smart Hosts*

Middle Boxes

CC Image courtesy of BiblioArchives / LibraryArchives
http://www.flickr.com/photos/lac-bac/8056743490/sizes/o/in/photostream/

Boxes in the middle of the network that try to make it smart

- NATs
- (TCP) Performance Enhancing Proxies
- Network Firewalls
- IDS/IPS
- Web Proxies
- P2P Caches

“All these middle boxes optimise current applications at the expense of future applications.”

(RFC6182)

Middle boxes make deploying changes to existing protocols or deploying new protocols hard

CC Image courtesy of Steven Depolo
http://www.flickr.com/photos/stevendepolo/3212039475/sizes/z/in/photostream/

CC Image courtesy of Tracey Adams a.k.a. bikracer
http://tinyurl.com/pnnqoxf

They can drop or damage packets they don't understand

Datagram Congestion Control Protocol (DCCP)

”Congestion Controlled UDP“

Better for both network and applications

Protocol number 33 (UDP is 17)

IPv4 NATs likely to drop it

Evading Middle Boxes

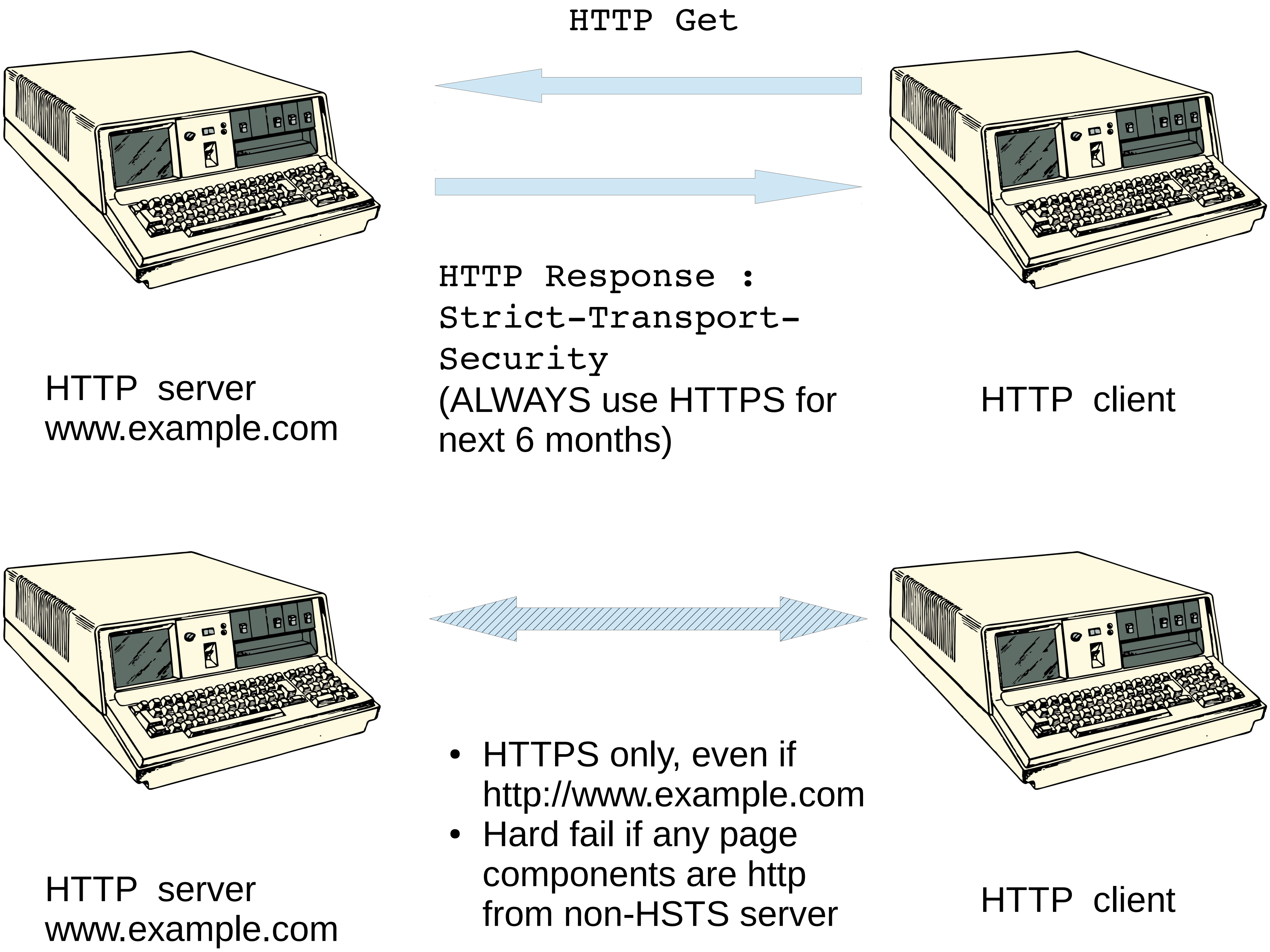
Look like what they know

Use covert channels and indirection

CC Image courtesy of colin houston a.k.a. col.hou
http://www.flickr.com/photos/colhou/4633274118/sizes/z/in/photostream/

HTTP Strict Transport Security (HSTS)

CC Image courtesy of kelp
http://www.flickr.com/photos/kelp/167089710/sizes/z/in/photostream/



HTTP Get

HTTP Response : Strict-Transport-Security
(ALWAYS use HTTPS for next 6 months)

HTTP server
www.example.com

HTTP client

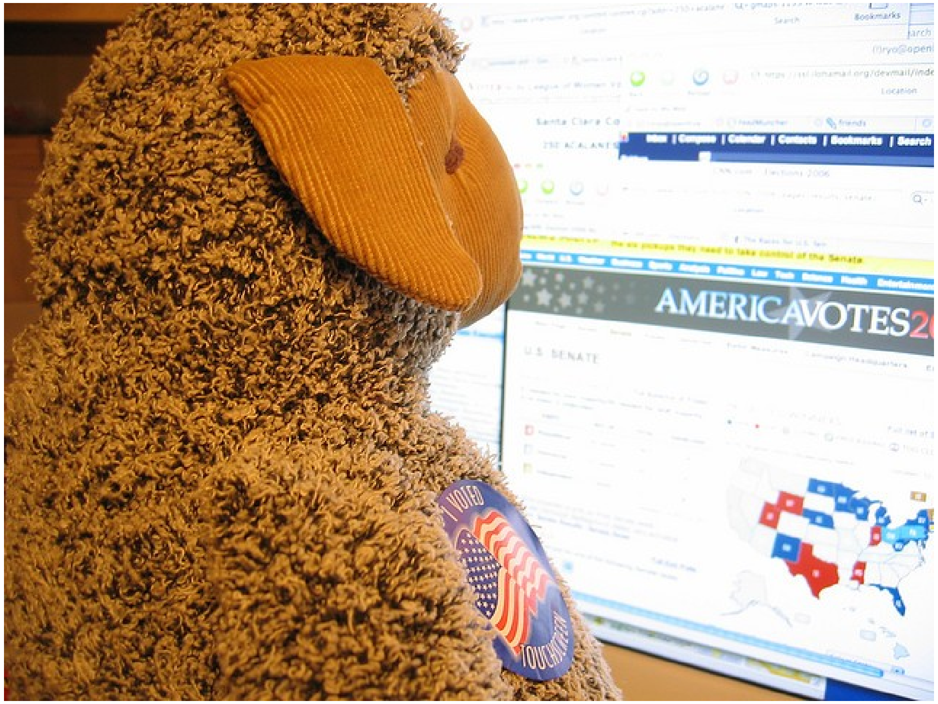
- HTTPS only, even if http://www.example.com
- Hard fail if any page components are http from non-HSTS server

HTTP server
www.example.com

HTTP client

A reaction to the Firesheep Firefox extension

It sniffed and then reused unencrypted cookies for unauthorised access to Facebook etc.



CC Image courtesy of Ryo Chijiiwa a.k.a. Ryochiji
http://www.flickr.com/photos/ryochijiiwa/291996188/sizes/z/in/photostream/

Unencrypted cookies were typically sniffed off of WEP (Wired Equivalent Privacy) protected public Wi-Fi Networks

Yeah, WEP **protected**

CC Image courtesy of Newsbie Pix
http://www.flickr.com/photos/newsbiepix/4336214968/sizes/z/in/photostream/

CC Image courtesy of Scott Hingst a.k.a. shingst
http://www.flickr.com/photos/shingst/4759579496/sizes/l/in/photostream/

So much for trusting the network to protect you

Our friend Charles-Guillaume might say,

"One is never served so well as by oneself, so don't rely on network protection, and use HSTS."

HSTS Implementations

Chromium and Google Chrome

Firefox

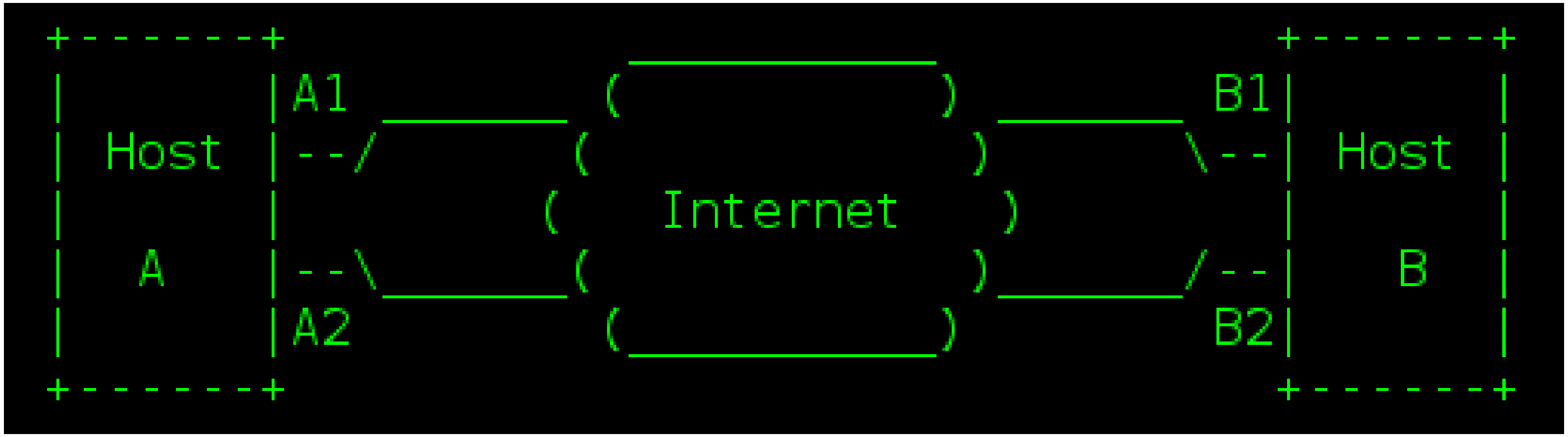
Opera

~~Safari~~

~~Internet Explorer~~

Multipath TCP (MPTCP)

CC Image courtesy of Robbie Sproule a.k.a. Robbie1
http://www.flickr.com/photos/robbie1/4359491/sizes/l/in/photostream/

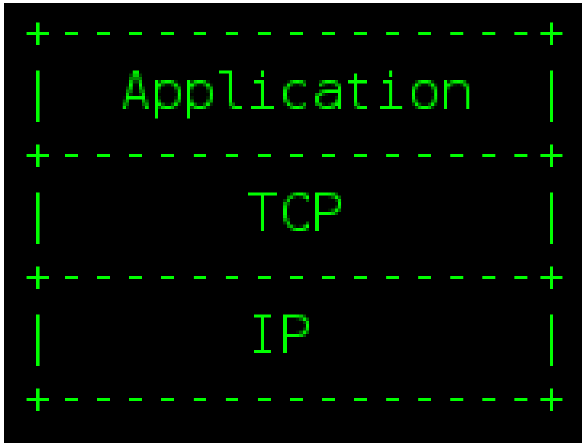


```
+-------+            __________             +-------+
|       |A1 ______  (          ) ______  B1|       |
| Host  |--/       (            )       \--| Host  |
|       |         (   Internet   )         |       |
|  A    |--\______ (            ) ______/--|   B   |
|       |A2         (__________)         B2|       |
+-------+                                   +-------+
```

RFC6182

Two hosts, Four paths

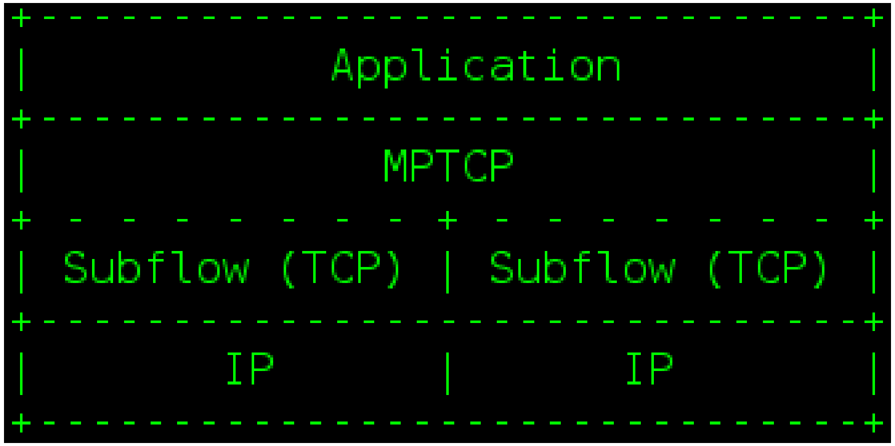
A1-B1, A1-B2, A2-B1, A2-B2



```
+---------------+
|  Application  |
+---------------+
|      TCP      |
+---------------+
|      IP       |
+---------------+
```

RFC6182

Standard TCP stack



```
+-------------------------------+
|           Application         |
+-------------------------------+
|             MPTCP             |
+ - - - - - - - + - - - - - - - +
| Subflow (TCP) | Subflow (TCP) |
+-------------------------------+
|       IP      |      IP       |
+-------------------------------+
```

RFC6182

Multipath TCP stack

Hosts announce MPTCP support to each other using new MP_CAPABLE TCP option

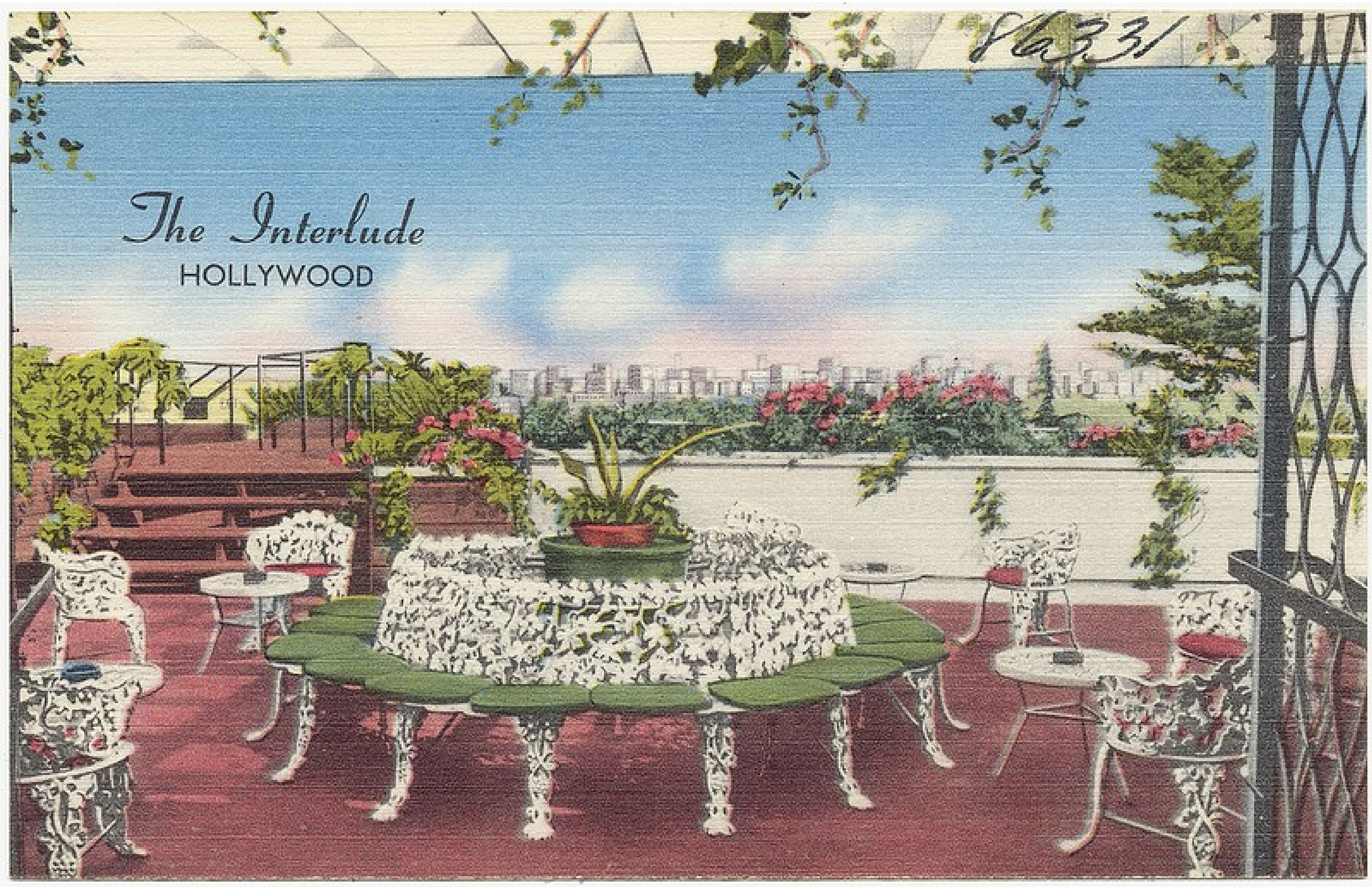
This first connection becomes the first Subflow

The MPTCP connection is identified using a 32 bit token

Additional Subflows supply the MPTCP connection token

If there are multiple Subflows between hosts, data is spread across them

Brief Interlude



CC image courtesy of Boston Public Library
http://www.flickr.com/photos/boston_public_library/7535891
370/sizes/c/in/photostream/

Subflows can be added when host interfaces come up

Or go away when a host interface goes down

Subflows look like TCP, to evade Middle Boxes

Subflows can be established over IPv4 or IPv6, regardless of what the application uses

Subflows can be flagged as a “backup path”, used if there are no “regular path” Subflows

What does this all mean?

Hosts and TCP applications get

Better Throughput

Better Resiliance

Basic IPv6 for IPv4 applications

Basic IPv4 for IPv6 applications

Our good friend Charles-Guillaume might say,

"One is never served so well as by oneself, so use all the networks.”

MPTCP Implementations

(draft-eardley-mptcp-implementations-survey)

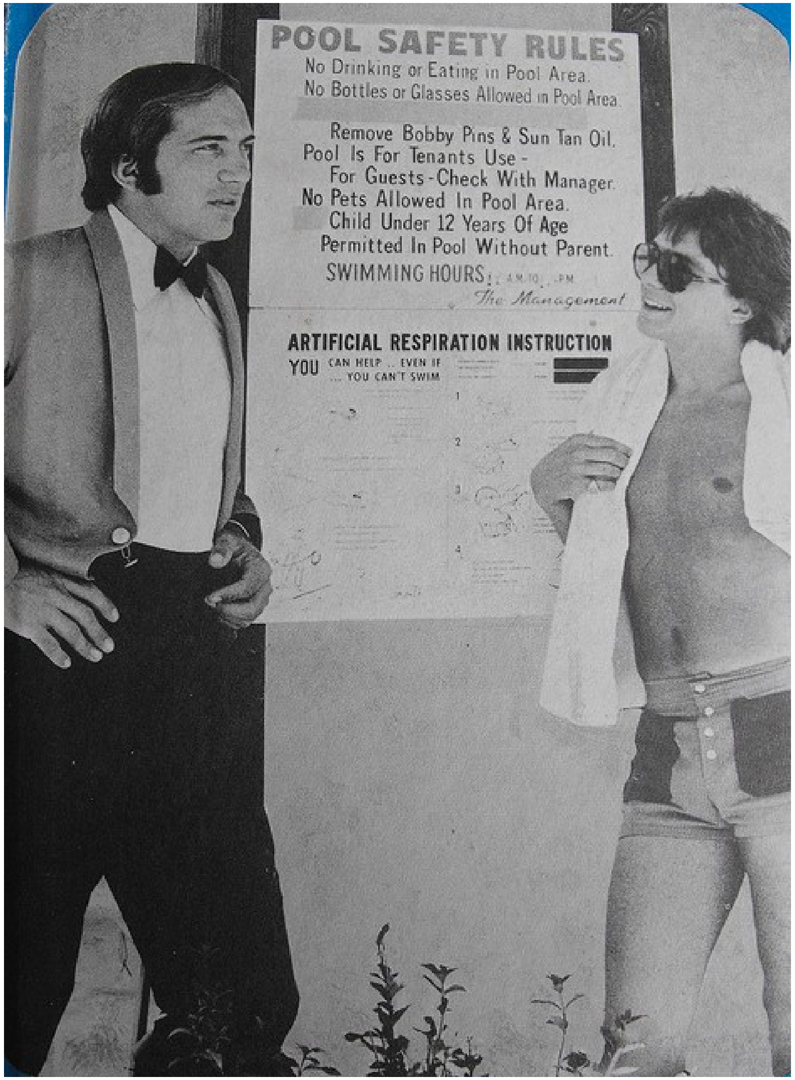
Linux implementation from UCLouvain

FreeBSD implementation from our friends at Swinburne

anonymous implementation in a commercial OS

NetScaler Firmware implementation from Citrix Systems, Inc.

HSTS & MPTCP – Trend Indicators?


POOL SAFETY RULES
No Drinking or Eating in Pool Area.
No Bottles or Glasses Allowed in Pool Area.
Remove Bobby Pins & Sun Tan Oil.
Pool Is For Tenants Use -
For Guests-Check With Manager.
No Pets Allowed In Pool Area.
Child Under 12 Years Of Age
Permitted In Pool Without Parent.
SWIMMING HOURS: A.M. TO P.M.
The Management
ARTIFICIAL RESPIRATION INSTRUCTION
YOU CAN HELP ... EVEN IF ... YOU CAN'T SWIM
1
2
3
4

CC image courtesy of tiffany terry a.k.a. libertygrace0
http://www.flickr.com/photos/35168673@N03/4392781532/
sizes/z/in/photostream/

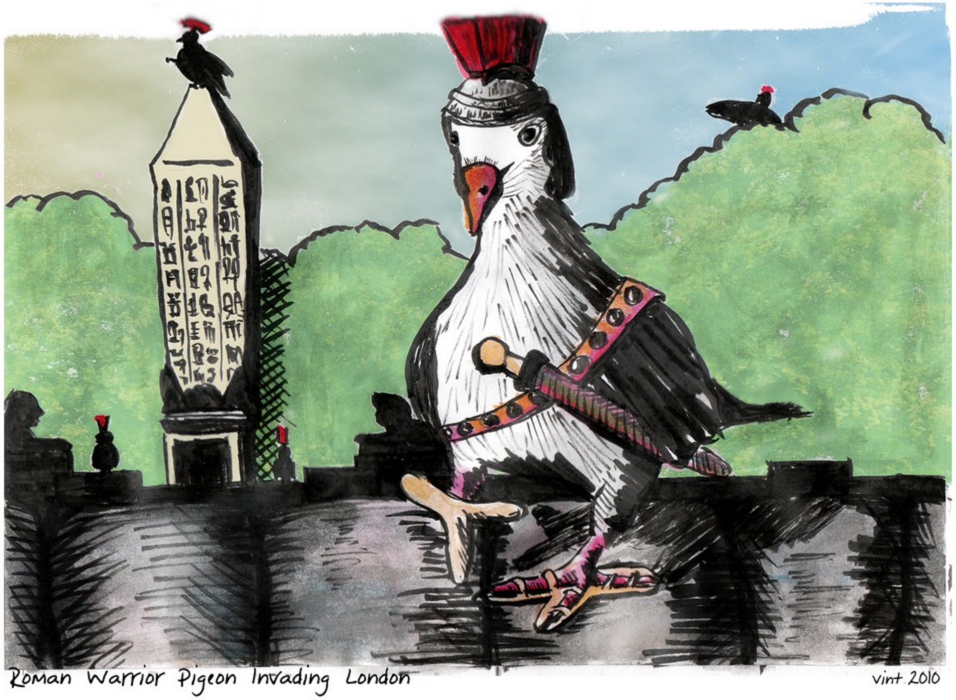
Host traffic encrypted more often

CC Image courtesy of kelp
http://www.flickr.com/photos/kelp/167089710/sizes/z/in/photostream/

CC Image courtesy of Robbie Sproule a.k.a. Robbie1
http://www.flickr.com/photos/robbie1/4359491/sizes/l/in/photostream/

Multipathing by hosts

More evidence of a trend?



CC image courtesy of vintagedept
http://www.flickr.com/photos/vintagedept/4361921235/sizes/
l/in/photostream/

RFC5386 - “**Better-Than-Nothing Security: An Unauthenticated Mode of Ipsec.**”
N. Williams, M. Richardson. **November 2008.**

And more?

“**Happy Eyeballs Extension for Multiple Interfaces**”, G. Chen, C. Williams, D. Wing, A. Yourtchenko, draft-ietf-mif-happy-eyeballs-extension

Impacts

CC image courtesy of Gemma Stiles
http://www.flickr.com/photos/gemmastiles/6927436488/sizes/c/in/photostream/

Current Traffic Assumptions

If a host is attached to our network, we'll see all of its traffic

(single homed)

Traffic is usually not encrypted

IPv4 applications only send IPv4 traffic

IPv6 applications only send IPv6 traffic

Current Traffic Assumptions

~~If a host is attached to our network, we'll see all of its traffic~~

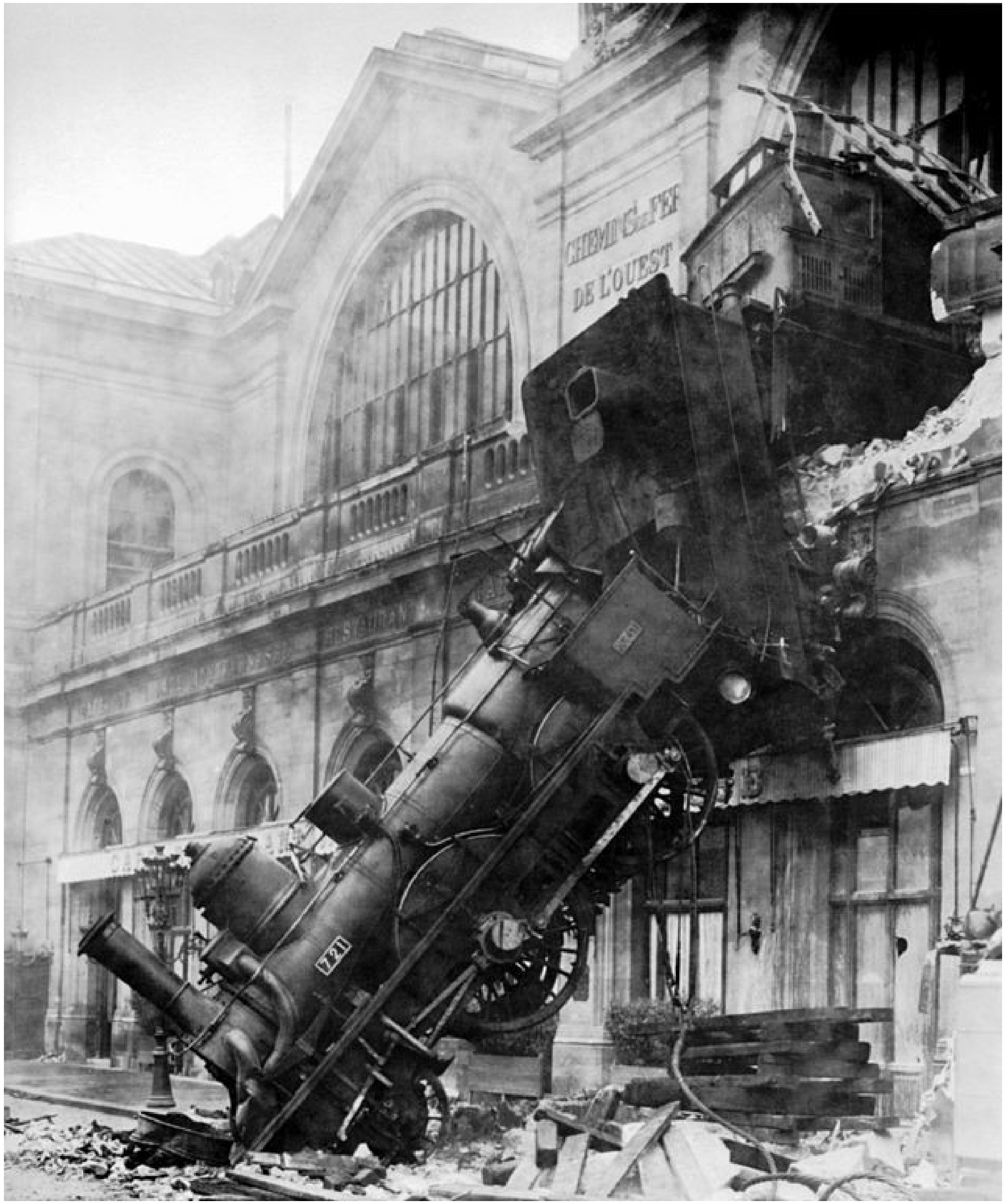
~~(single homed)~~

~~Traffic is usually not encrypted~~

~~IPv4 applications only send IPv4 traffic~~

~~IPv6 applications only send IPv6 traffic~~

It's a Geoff Huston scale train wreck!



http://en.wikipedia.org/wiki/Montparnasse_derailment

Trouble for Middle Boxes?

Middle Boxes won't see all the traffic, so they might

- **Break host communications** (fortunately there is an alternate path)
- **Go transparent**, making them valueless
- **Degrade hosts' throughput**, perhaps badly (fortunately there is an alternate path)

Trouble for Troubleshooting?

CC image courtesy of Michael 1952
http://www.flickr.com/photos/mike52ad/4781531593/sizes/l/in/photostream/

We won't be able to rely on seeing all the host's traffic inside the network

Better troubleshooting tools and methods on hosts will need to be developed

Trouble for VPNs?

Multipathing may cause to-be-secured traffic to leak outside the VPN

Traffic should be secured (encrypted) on the host itself

Any point to VPNs if hosts encrypt everything?

CC image courtesy of Daniel X. O'Neil a.k.a. Danxoneil
http://www.flickr.com/photos/juggernautco/8314485754/sizes/l/in/photostream/

Trouble for network QoS?

CC image courtesy of Steve Snodgrass
http://www.flickr.com/photos/stevensnodgrass/7390067836/
sizes/c/in/photostream/

Smarter hosts may or will “multipath” around congestion, also helping to reduce it

Is network QoS necessary after that?

So are there any bright sides?

Smarter hosts will probably reward networks that are dumb, fast and well interconnected

So we'll need to keep building them

So, to the final question

Santos tour down under 2010
JAYCO STAGE 5 • FINISH • WILLUNGA
ADELAIDE AUSTRALIA
0:00
2:16:55

CC image courtesy of Anthony Cramp
http://www.flickr.com/photos/anthonycramp/4314540519/sizes/l/in/photostream/

How likely are encryption and multipathing going to be implemented on MMHHs?

Is there an organisation who has the

- Motivation
- Capability and
- Resources

to have encryption and multipathing implemented on MMHHs, for the benefit of its customers?

Is there an organisation who

provides money making content,

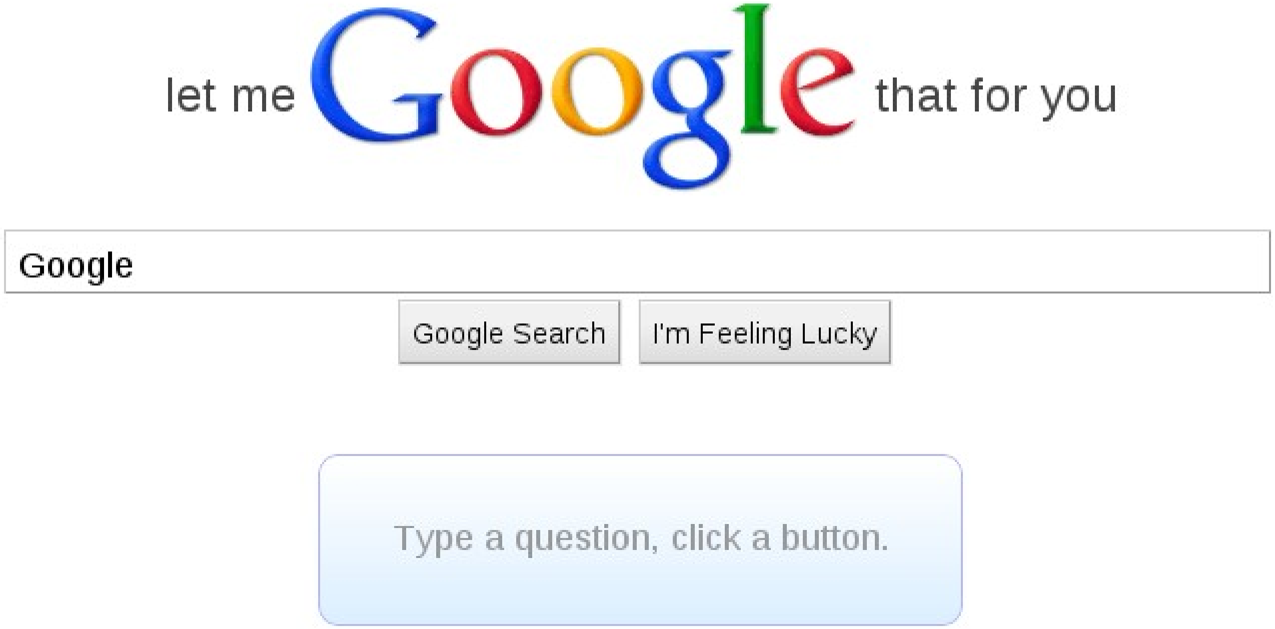
provides services where application traffic encryption over the network would be important,

and ...

leads the development of an OS for MMHHs?

So I'm guessing you've guessed who I've guessed.

But in case you haven't,



Google

Type a question, click a button.

Questions?

CC image courtesy of Kiwithing
http://www.flickr.com/photos/kiwisaotome/8261132558/sizes/c/in/photostream/

Thanks for listening