

twitter @axelarnbak

De Wereldreis van een Facebook Update
Over de werking en beveiliging van het internet

Axel Arnbak, LL.M.

15 mei 2013, Internet Workshop @ Tweede Kamer

<http://www.ivir.nl/medewerkers/arnbak.html>

'Het Internet'? 'Cyberspace'?



'Cybersecurity'? 'Cloud'?

Topje ijsberg



OUTLINE

“Het Internet”: netwerk van netwerken

De wereldreis van één Facebook update

Beveiligingshobbels onderweg

Systeembeveiliging: Botnets & DDoS

OUTLINE

“Het Internet”: netwerk van netwerken

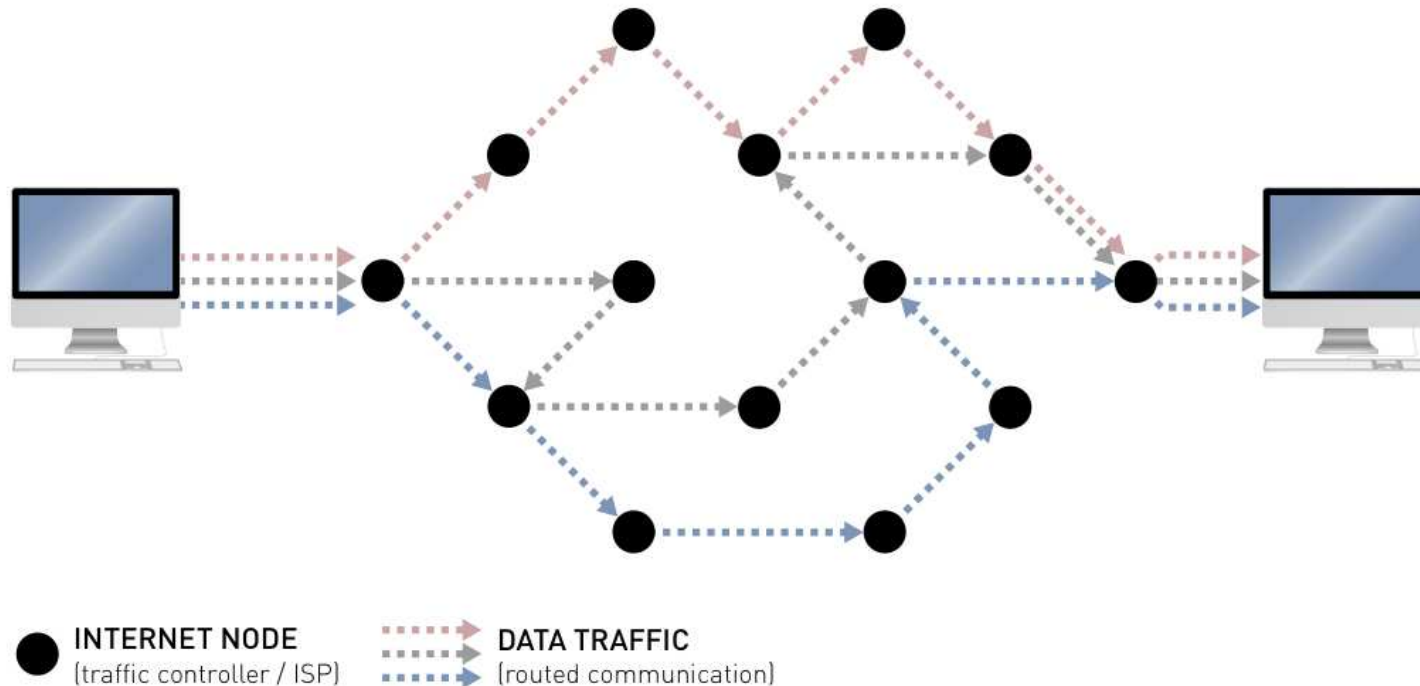
De wereldreis van één Facebook update

Beveiligingshobbels onderweg

Systeembeveiliging: Botnets & DDoS

THE INTERNET

A NETWORK OF COMPUTER NETWORKS

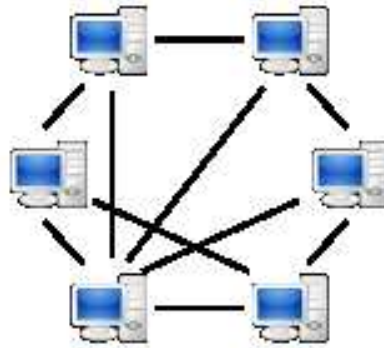


Taal = Internet Protocol (ca. 1974)

talloze applicaties gebaseerd op IP

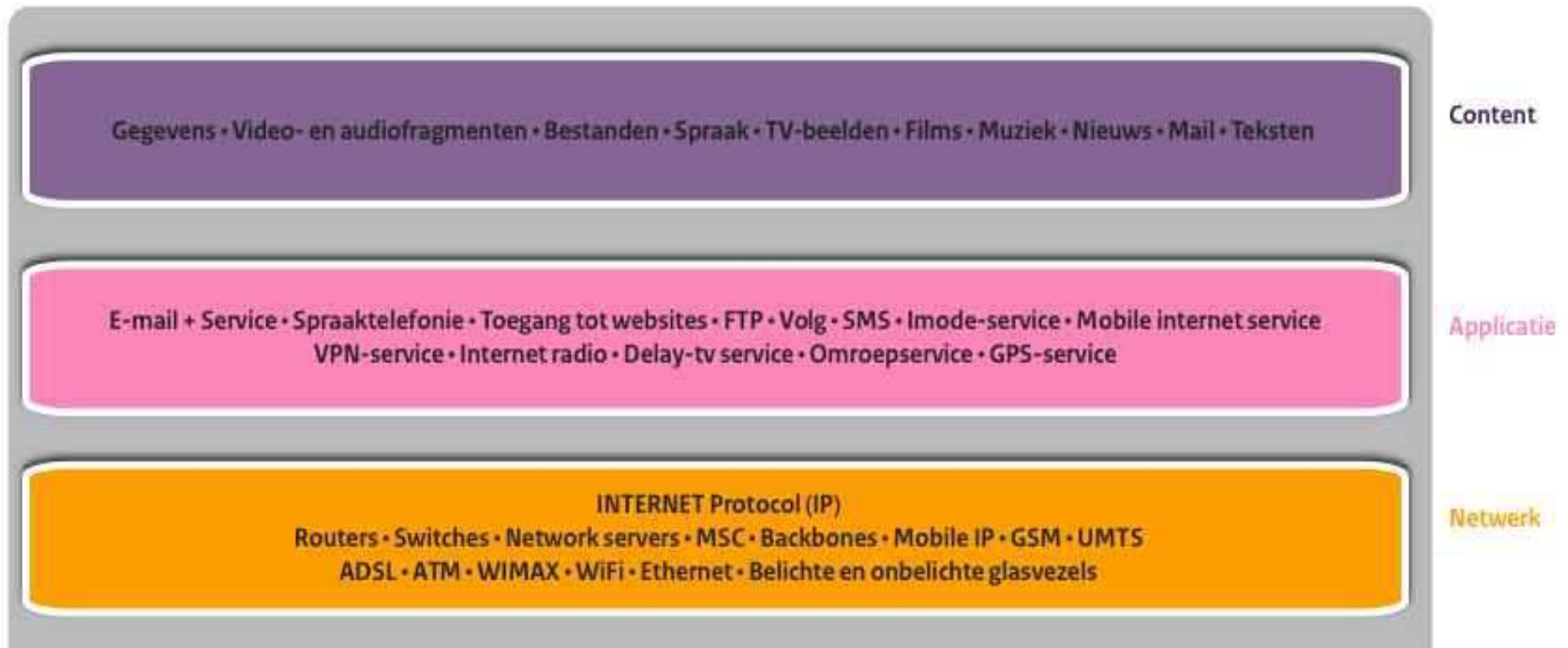


! internet $\Leftrightarrow$ web



kern succes = openheid/flexibiliteit

Lagenmodel: Content – Applicatie – Netwerk



[simplificatie]



domesticatie

OUTLINE

“Het Internet”: netwerk van netwerken

De wereldreis van één Facebook update

Beveiligingshobbels onderweg

Systeembeveiliging: Botnets & DDoS



FAVORITES

- Welcome
- News Feed
- Messages
- Events
- Photos
- Find Friends

FRIENDS

- Close Friends
- Family

APPS

- App Center
- Games Feed
- Music
- Notes
- Links
- Pokes

PAGES

- Like Pages

Update Status Add Photos/Video

Dag lieve mensen



Public

Post

SORT

There are no more posts to show right now.

Find More Friends

by the Friends



Find Friends

Facebook © 201

English (US) · Privacy
More

Eén Facebook update...

... Gaat op wereldreis





FAVORITES

- Welcome
- News Feed
- Messages
- Events
- Photos
- Find Friends

FRIENDS

- Close Friends
- Family

APPS

- App Center
- Games Feed
- Music
- Notes
- Links
- Pokes

PAGES

- Like Pages

Update Status Add Photos/Video

Dag lieve mensen



Public

Post

SORT

There are no more posts to show right now.

Find More Friends

by the Friends



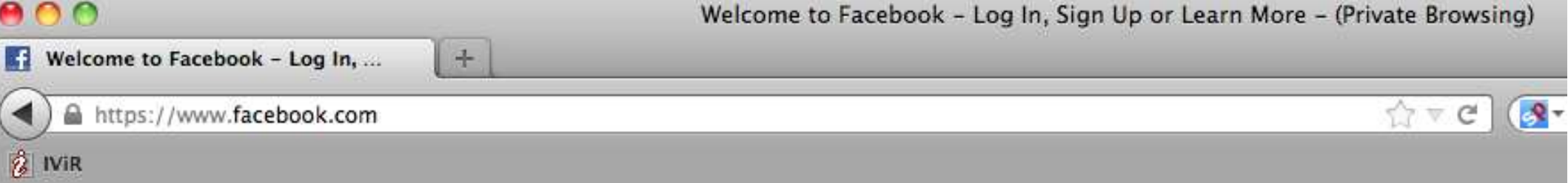
Find Friends

Facebook © 201

English (US) · Pri

More

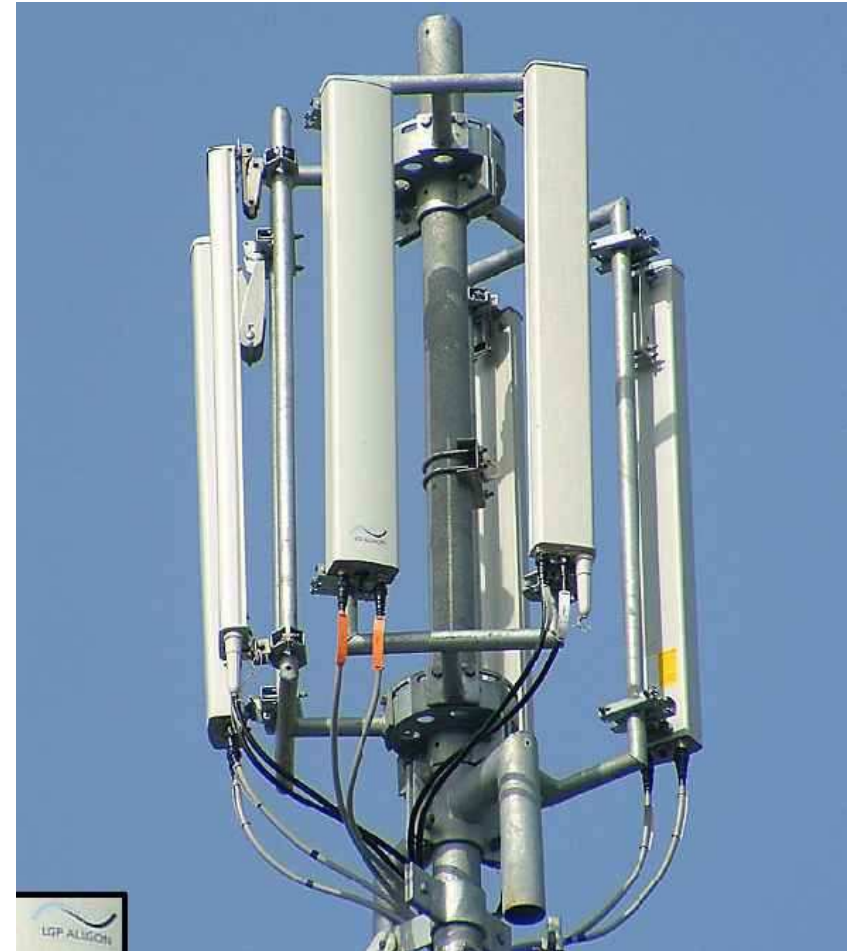
die update gaat langs...



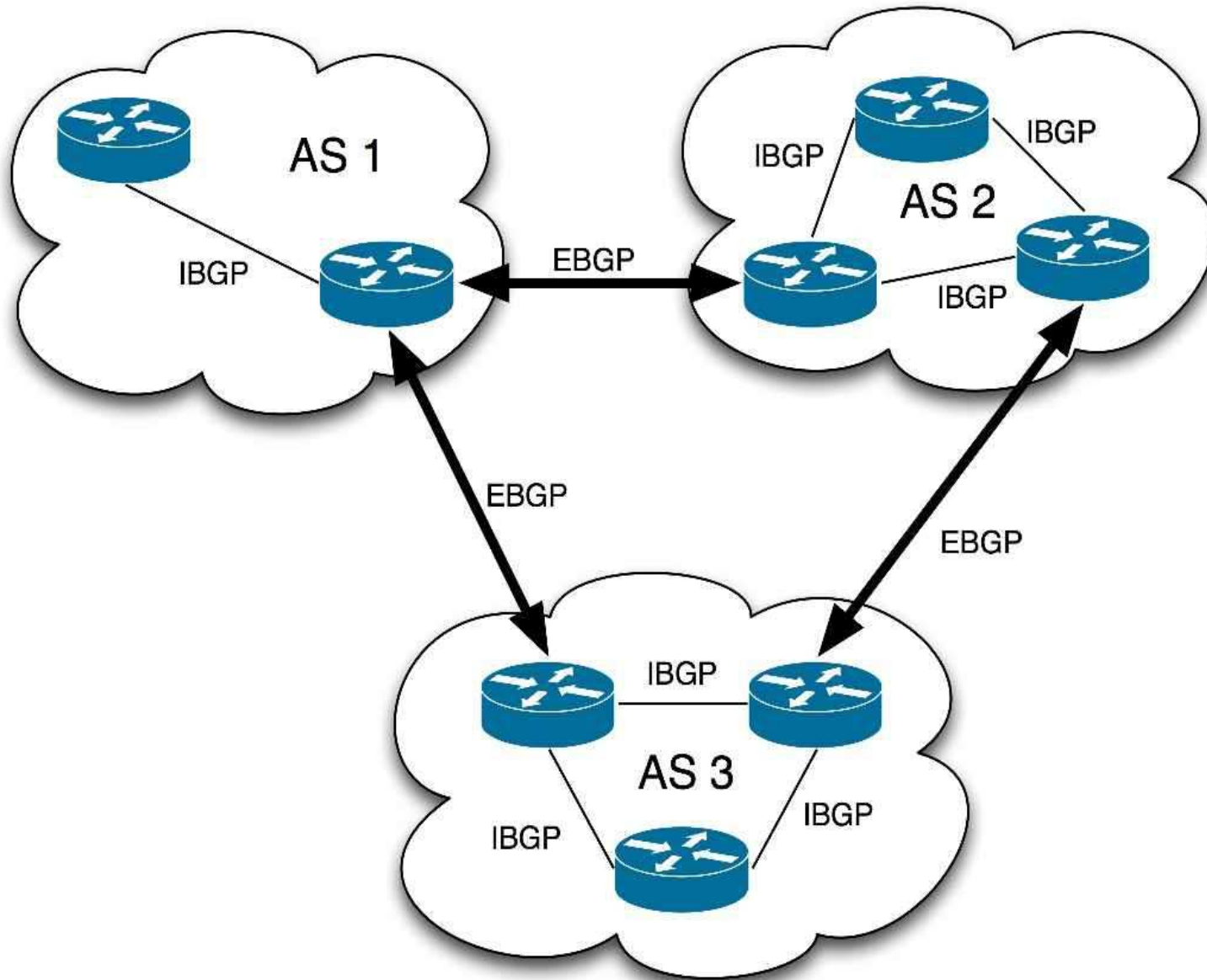
app of browser



router



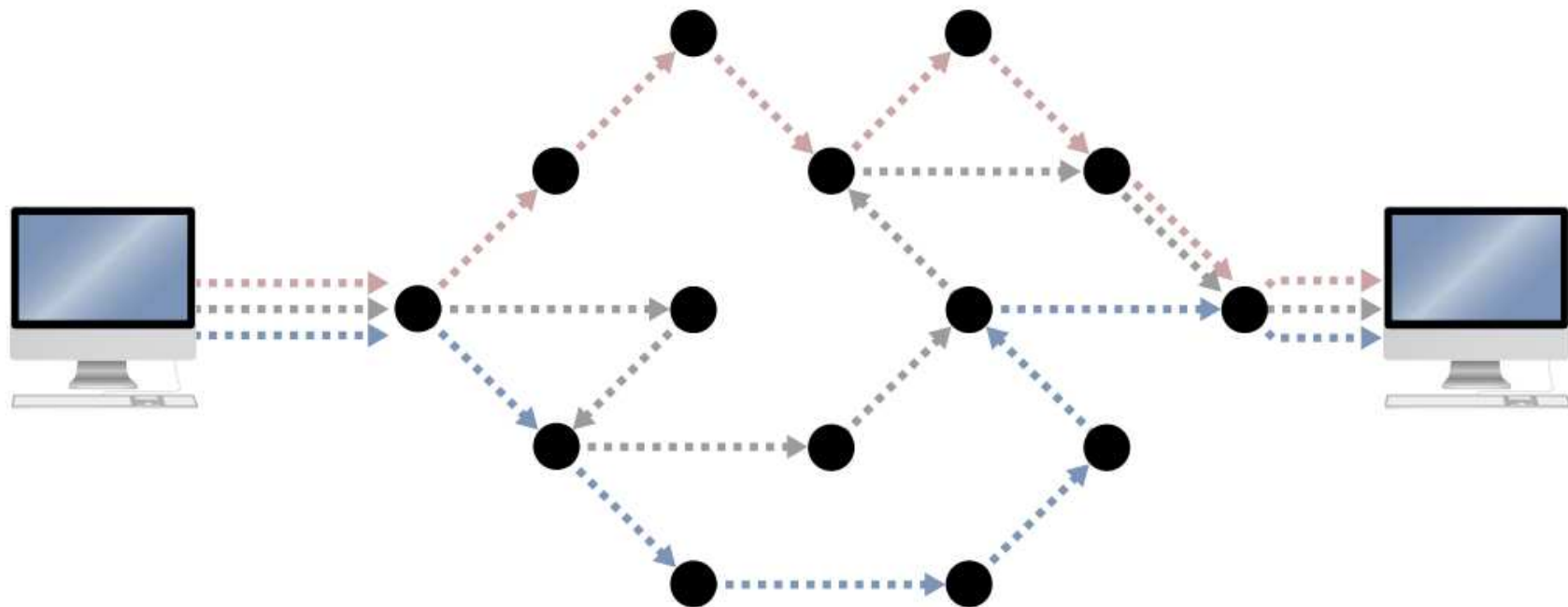
antenne



amsterdam internet exchange

THE INTERNET

A NETWORK OF COMPUTER NETWORKS



INTERNET NODE
(traffic controller / ISP)

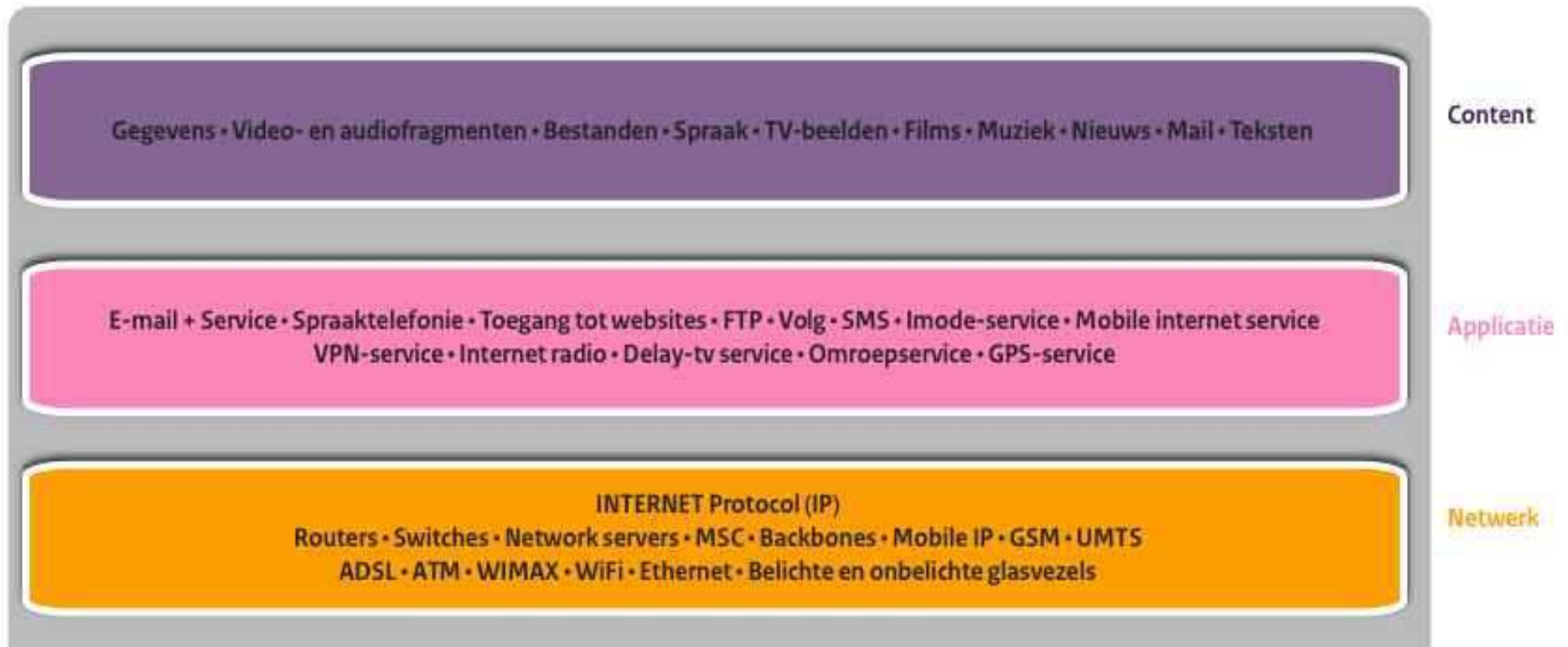


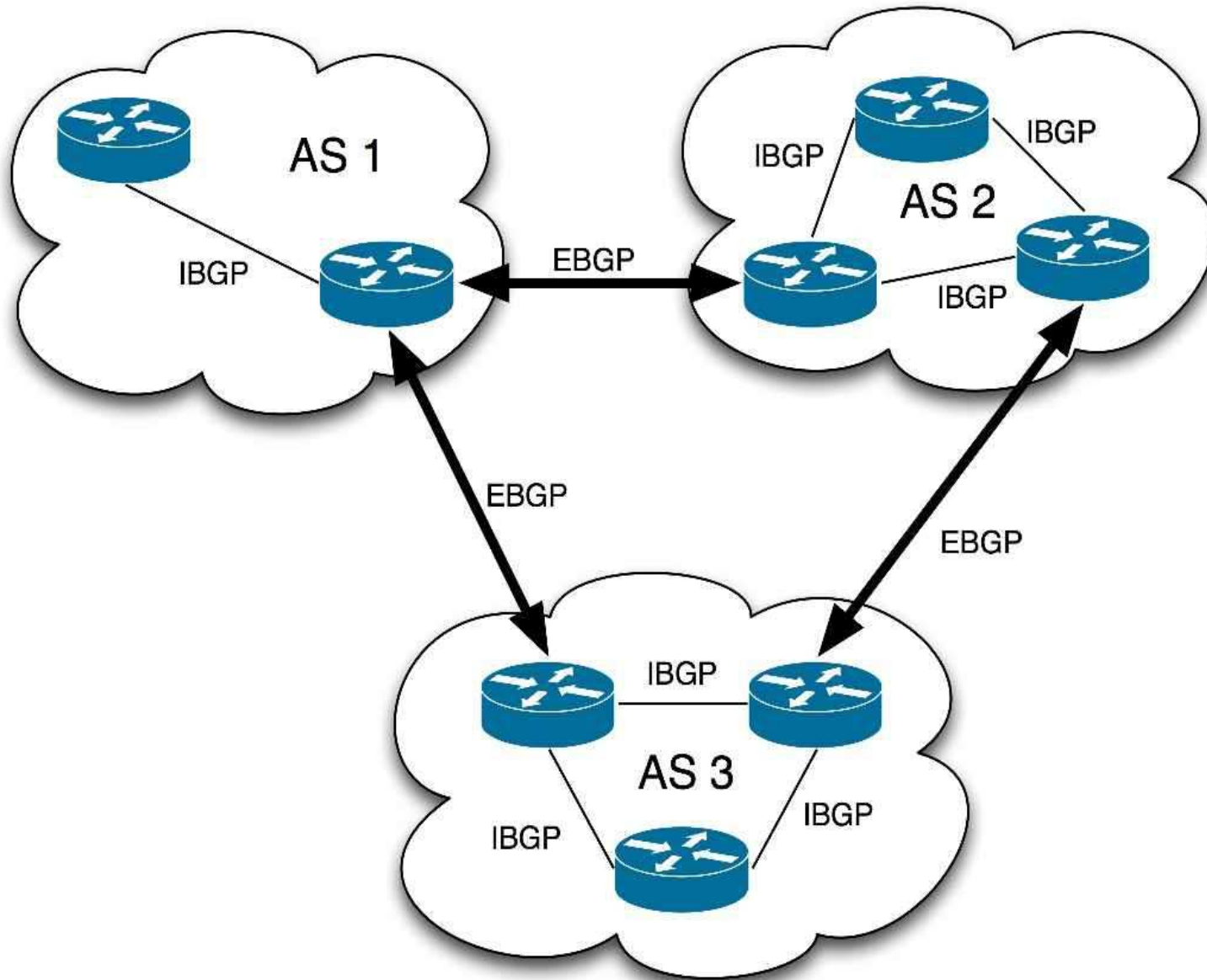
DATA TRAFFIC
(routed communication)

A photograph of a server room with blue lighting. Rows of server racks are visible, with some racks having glass doors that show internal components. The room has a high ceiling with exposed pipes and cables. The overall atmosphere is futuristic and high-tech.

Servers van Facebook

de reis doorloopt het lagenmodel





network = AMS-IX



netwerk = antenne/router



applicatie =
app of browser



FAVORITES

- Welcome
- News Feed**
- Messages
- Events
- Photos
- Find Friends

FRIENDS

- Close Friends
- Family

APPS

- App Center
- Games Feed
- Music
- Notes
- Links
- Pokes

PAGES

- Like Pages

Update Status Add Photos/Video

Dag lieve mensen



Public

Post

SORT

There are no more posts to show right now.

Find More Friends

the Fri



Find Friends

Facebook © 201

English (US) · Pri
More

content = update

Traceroute IPv4

www.facebook.com

Start

```
traceroute to star.c10r.facebook.com (173.252.112.23), 30 hops max, 52 byte
 1 v867.router1.dcg.transip.net (80.69.67.220) 26.731 ms
 2 br01.ams1.tfbnw.net (195.69.145.115) 0.729 ms
 3 ae1.bb02.ams2.tfbnw.net (31.13.29.90) 0.874 ms
 4 ae3.bb02.lhr2.tfbnw.net (31.13.30.131) 8.973 ms
 5 be5.bb01.dca1.tfbnw.net (31.13.31.2) 84.734 ms
 6 ae36.bb02.iad1.tfbnw.net (31.13.29.176) 108.634 ms
 7 ae0.dr03.ash3.tfbnw.net (204.15.21.104) 84.413 ms
 8 *
 9 edge-star-shv-03-ash5.facebook.com (173.252.112.23) 83.607 ms
```

Traceroute laat het netwerkpad tussen twee locaties zien. Met traceroute bekijkt u welk pad internetverkeer volgt van het TransIP netwerk naar uw adres.

Terminal Shell Edit View Window Help

Terminal — traceroute — 178x53

Last login: Tue May 14 16:55:48 on ttys000

admins-macbook:~ admin\$ traceroute www.facebook.com

```
traceroute to star.c10r.facebook.com (31.13.64.1), 64 hops max, 52 byte packets
 1      }.178.1) 3.918 ms 2.538 ms 2.414 ms
 2 lo1.dr8.d12.xs4all.net (194.109.5.205) 22.944 ms 20.680 ms 21.672 ms
 3 1418.ae3.xr4.1d12.xs4all.net (194.109.7.17) 25.650 ms 22.043 ms 20.985 ms
 4 0.so-0-2-0.xr1.tc2.xs4all.net (194.109.5.10) 21.433 ms
   0.ge-0-2-0.xr1.sara.xs4all.net (194.109.5.2) 22.973 ms
   0.so-0-2-0.xr1.tc2.xs4all.net (194.109.5.10) 20.468 ms
 5 br02.ams1.tfbnw.net (195.69.145.164) 20.753 ms 21.256 ms
   br01.ams1.tfbnw.net (195.69.145.115) 21.222 ms
 6 ae2.bb02.ams2.tfbnw.net (31.13.29.92) 23.864 ms
   po126.msw01.01.ams2.tfbnw.net (31.13.24.57) 41.227 ms 21.934 ms
 7 ae1.pr01.ams2.tfbnw.net (31.13.29.91) 22.847 ms *
   ae0.pr01.ams2.tfbnw.net (31.13.29.87) 21.927 ms
```

traceroute

OUTLINE

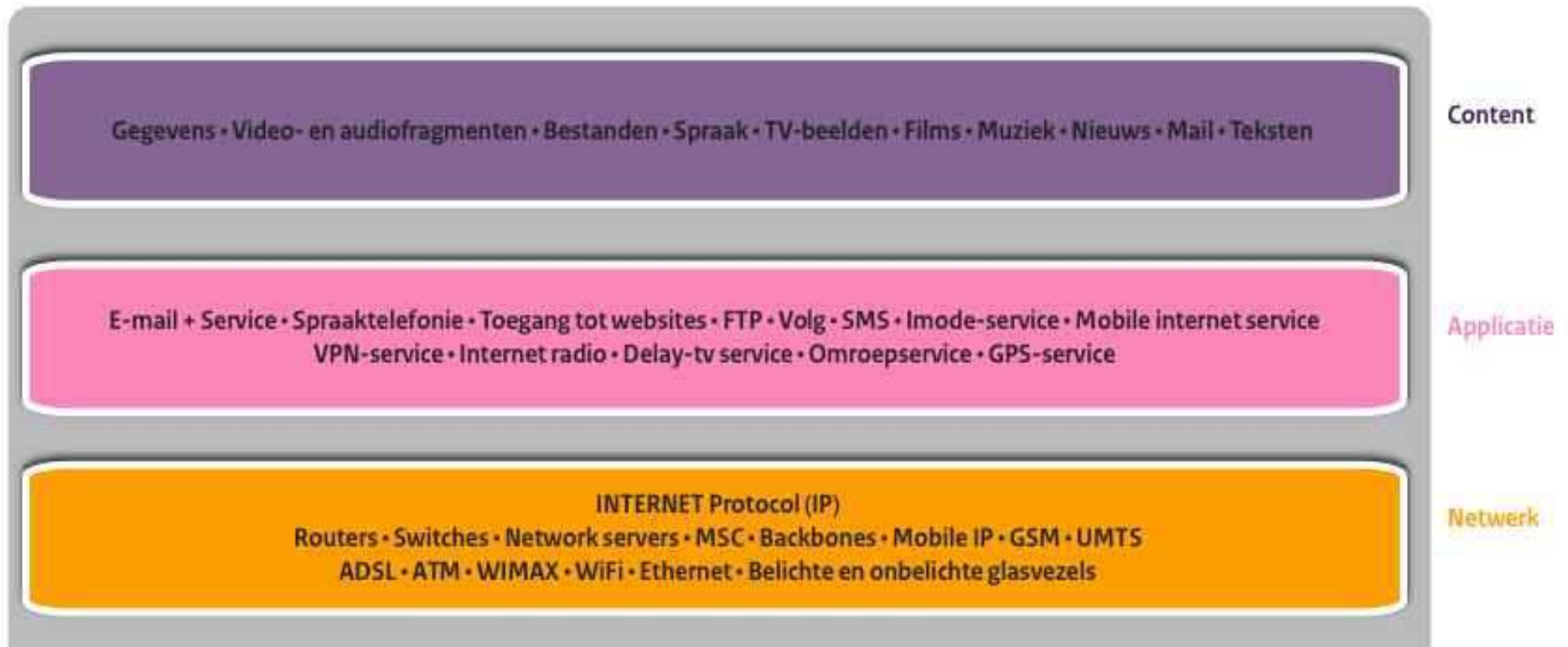
“Het Internet”: netwerk van netwerken

De wereldreis van één Facebook update

Beveiligingshobbels onderweg

Systemebeveiliging: Botnets & DDoS

beveiligingshobbels in iedere laag



Search

[Home](#) [Business](#) [Investing](#) [Technology](#) [Entrepreneurs](#) [Op/Ed](#)

Special Report

Cisco's Backdoor For Hackers

Andy Greenberg, 02.03.10, 01:45 PM EST

The methods networking companies use to let the Feds watch suspects also expose the rest of us.

ARLINGTON, Va. -- Activists have long grumbled about the privacy implications of the legal "backdoors" that networking companies like **Cisco** build into their equipment--functions that let law enforcement quietly track the Internet activities of criminal suspects. Now an **IBM** researcher has revealed a more serious problem with those backdoors: They don't have particularly strong locks, and consumers are at risk.

network: routers

Huawei

The company that spooked the world

The success of China's telecoms-equipment behemoth makes spies and politicians elsewhere nervous

Aug 4th 2012 | SAN FRANCISCO AND SHENZHEN | from the print edition



Enable Facebook



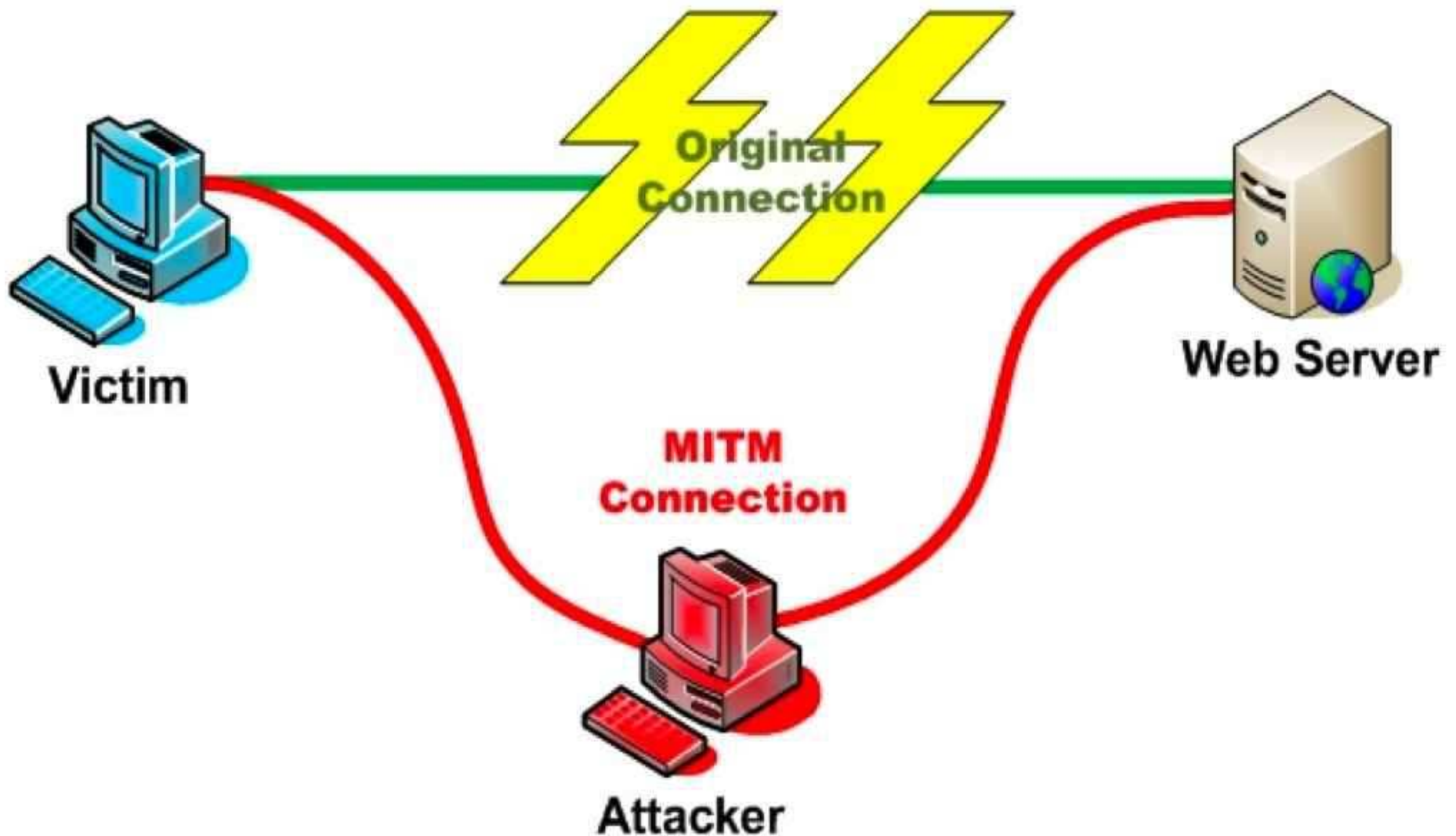
Tweet 7

network: antennae

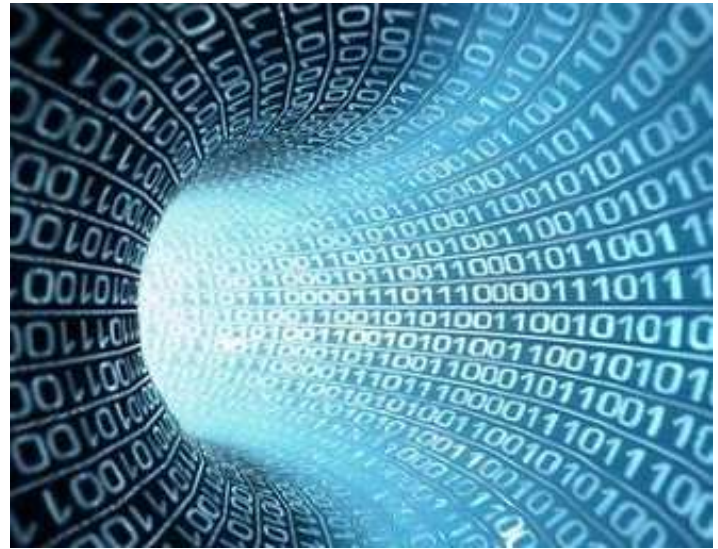
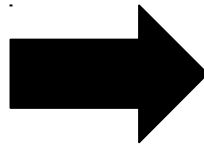
applicatie: browser







meeluisteren op de lijn



https://www.



zeker weten met wie u via
internet afspraken maakt

www.diginotar.nl



DigiNotar
Internet Trust Services

...sche handtekening

cybercrime bijproduct matige beveiliging

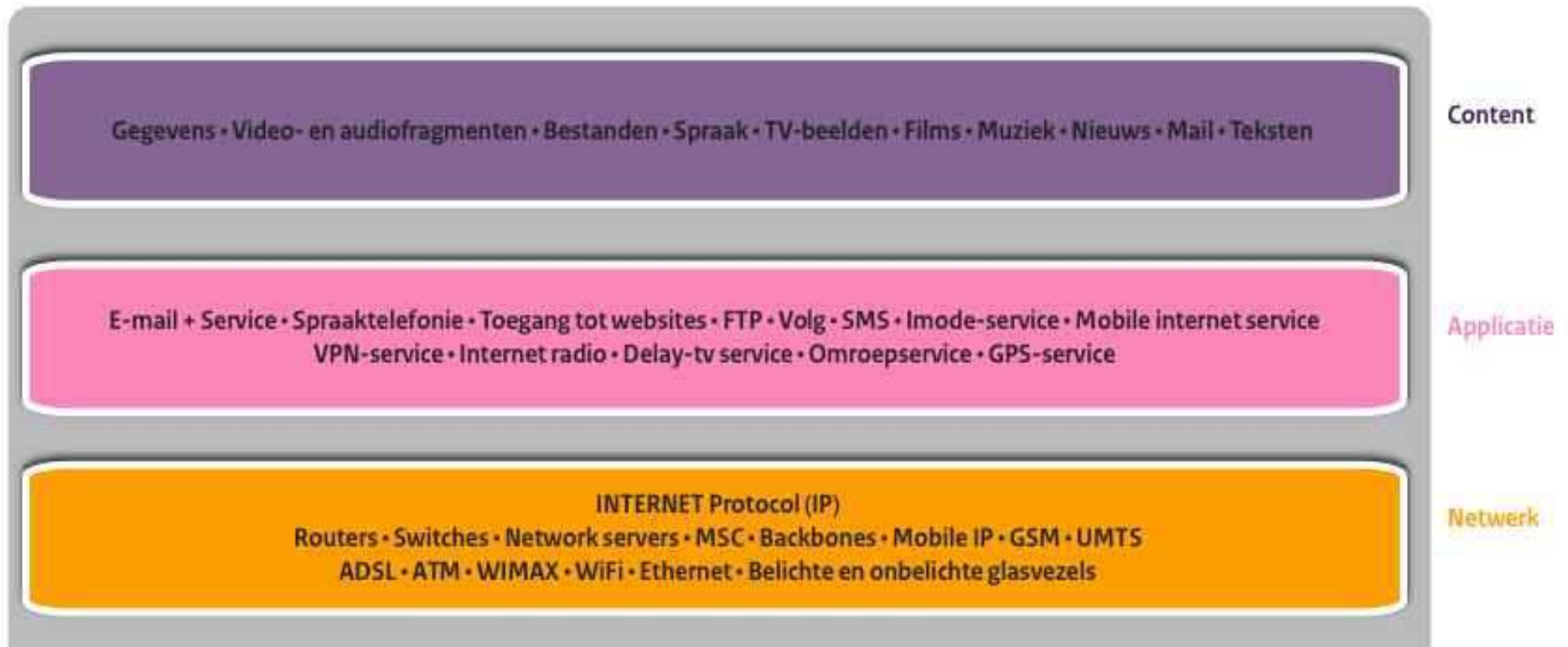
Where Do All The Attacks Go?

Dinei Florêncio and Cormac Herley
Microsoft Research
One Microsoft Way
Redmond, WA, USA

“Many attacks cannot be made profitable, even when many profitable targets exist.”

https aanvallen geavanceerd, consensus: staten

waar waren we ook alweer?



A photograph of a server room with blue lighting. Rows of server racks are visible, with some racks having glass doors that show internal components. The room has a high ceiling with exposed pipes and cables. The overall atmosphere is futuristic and high-tech.

Servers van Facebook



FAVORITES

- Welcome
- News Feed
- Messages
- Events
- Photos
- Find Friends

FRIENDS

- Close Friends
- Family

APPS

- App Center
- Games Feed
- Music
- Notes
- Links
- Pokes

PAGES

- Like Pages

Update Status Add Photos/Video

Dag lieve mensen



Public

Post

SORT

There are no more posts to show right now.

Find More Friends

the Fri



Find Friends

Facebook © 201

English (US) · Pri
More

content = update



No account status changes.

Account status changes

Active Sessions

Address Book

Address

Apps You Admin

Pages You Admin

Administrative Records

Ad Clicks

Ads Topics

Alternate Name

Apps

Birthday Visibility

City and Hometown Info

Currency

Deleted Friends

Education

Emails

Events Info

wat slaat FB op? [1]

Deleted Friends
Education
Emails
Events Info
Facial Recognition Data
Family Members
Hidden From News Feed
Pending Friend Requests
Spoken Languages
Locale
Login Info
Logouts Info
Networks
Notifications Settings
Phone Numbers
Physical Tokens
Poke Info
Previous Names
Recognized Devices
Relationship Info
Account Activity
Screennames

wat slaat FB op? [2]



Account status changes

Active Sessions

Address Book

Address

Apps You Admin

Pages You Admin

Administrative Records

Ad Clicks

Ads Topics

Alternate Name

Apps

Birthday Visibility

City and Hometown Info

Currency

Deleted Friends

Date	Event	IP Address	Datr	User Agent
Today at 3:53pm	Session updated	146.50.144.115	...BXR5	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.5; rv:16.0) Gecko/20100101 Firefox/16.0
Today at 2:57pm	Email Added	146.50.144.115	...BXR5	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.5; rv:16.0) Gecko/20100101 Firefox/16.0
Today at 2:57pm	Email Added	146.50.144.115	...BXR5	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.5; rv:16.0) Gecko/20100101 Firefox/16.0
Today at 2:57pm	Email Demoted	146.50.144.115	...BXR5	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.5; rv:16.0) Gecko/20100101 Firefox/16.0
Today at 2:52pm	Login	146.50.144.115	...BXR5	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.5; rv:16.0) Gecko/20100101 Firefox/16.0
Today at 2:51pm	Web Session Terminated	146.50.144.115	...BXR5	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.5; rv:16.0) Gecko/20100101 Firefox/16.0
Today at 2:44pm	Login	146.50.144.115	...BXR5	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.5; rv:16.0) Gecko/20100101 Firefox/16.0

wat slaat FB op? [3]



Account status changes

Active Sessions

Address Book

Address

Apps You Admin

Pages You Admin

Administrative Records

Ad Clicks

Ads Topics

Alternate Name

Apps

Birthday Visibility

City and Hometown Info

Currency

Last IP Usage

IP	Time	Site
146.50.144.115	Today at 2:52pm	www.facebook.com
146.50.144.115	Today at 2:44pm	www.facebook.com

Login Protection Data

Type	Value	Date Added	Week Last Seen
datr	...BXR5	Today at 2:44pm	Today at 2:44pm
IP address	146.50.144.115	Today at 2:44pm	Today at 2:44pm
geolocation	52.368, 4.888	Today at 2:44pm	Today at 2:44pm

wat slaat FB op? [4]



geolocation 52.368, 4.888



Web

Afbeeldingen

Maps

Shopping

Meer ▾

Zoekhulpmiddelen

2 resultaten (0,09 seconden)

[De Krijtberg - Wikidi](#)

[wikidi.com](#) › [Building Category](#) - [Vertaal deze pagina](#)

De Krijtberg. Wikidi home Building Category De Krijtberg. Location. **Geolocation.**
4.88805555556 × 52.3677777778. Contained by, Netherlands · [Edit this page ...](#)

By ZACK WHITTAKER / CBS NEWS / December 4, 2012, 3:59 PM

Patriot Act can "obtain" data in Europe, researchers say



AP FILE

[3 Comments](#) / [Shares](#) / [Tweets](#) / [Stumble](#) / [Email](#)[More](#)

LONDON | European data stored in the "cloud" could be acquired and inspected by U.S. law enforcement and intelligence agencies, despite Europe's strong data protection laws, university researchers have suggested.

The research paper, titled "[Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act](#)," written by legal experts at the University of Amsterdam's Institute for Information Law, support previous reports that the anti-terror Patriot Act could be theoretically used by U.S. law enforcement to bypass

cloud computing
&
Patriot Act

OUTLINE

“Het Internet”: netwerk van netwerken

De wereldreis van één Facebook update

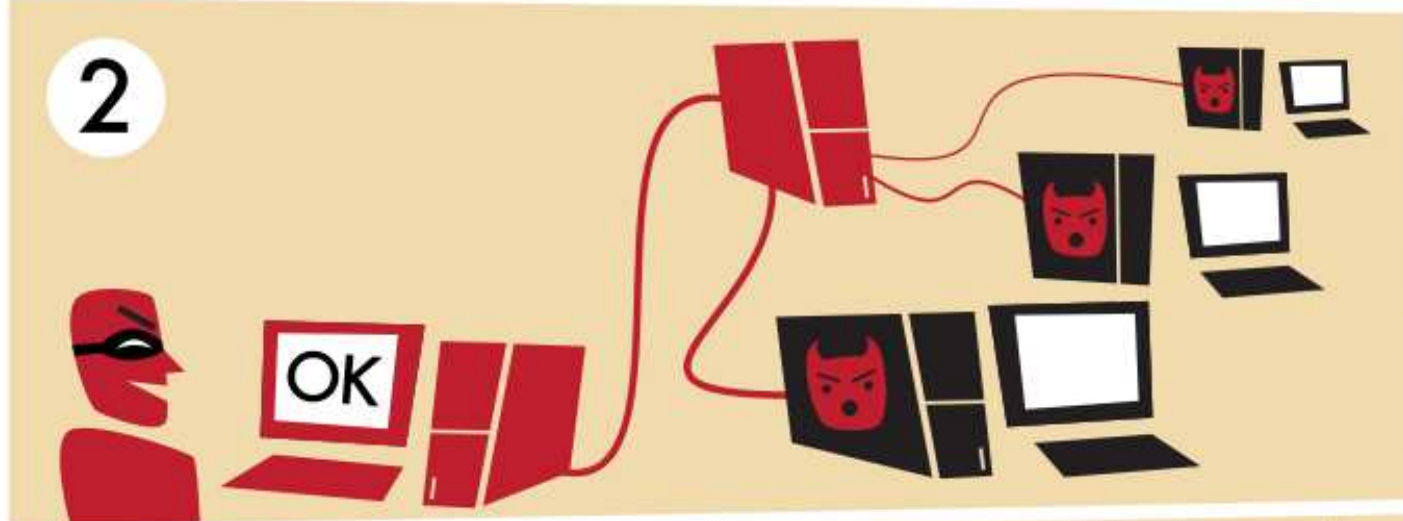
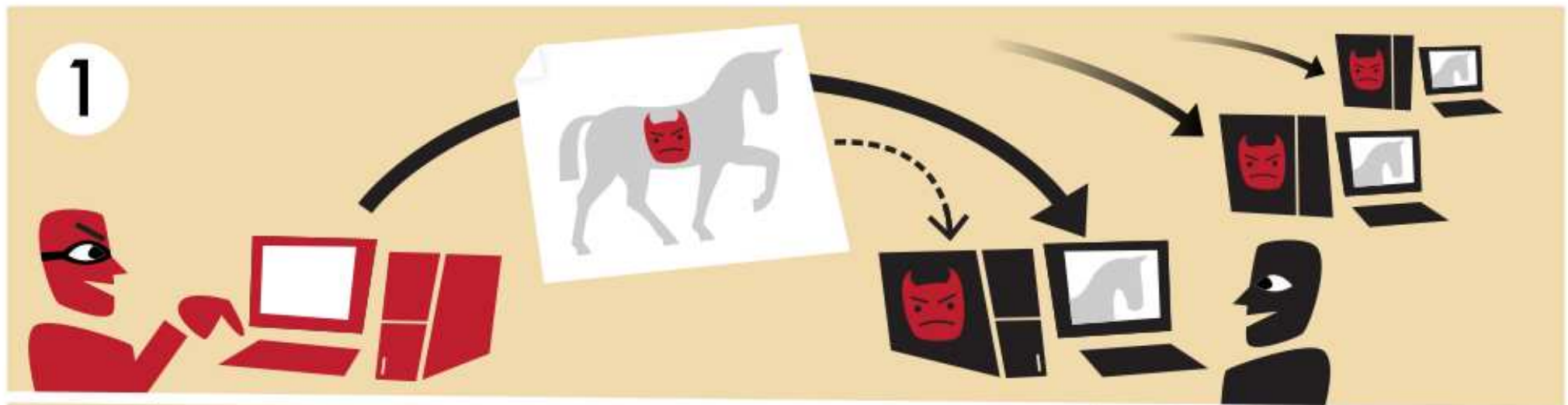
Beveiligingshobbels onderweg

Systeembeveiliging: Botnets & DDoS

netwerk van netwerken...



... connectiviteit én afhankelijkheid



DDoS





updates

geïnfecteerde gebruikers zijn overal ...



... hoe systeembeveiliging verbeteren?

monoculturen als risico



met schaal komt verantwoordelijkheid

Gadgetwise



Getting Smart About Personal Technology

April 19, 2013, 7:26 am | 10 Comments

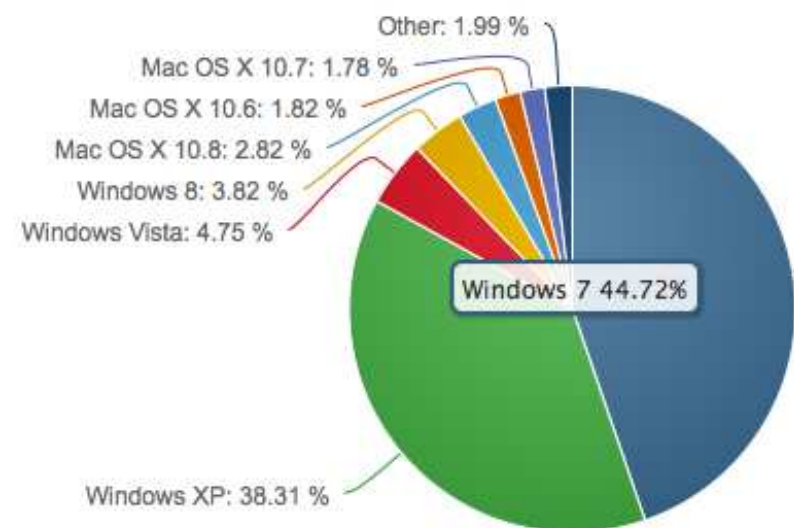
Q&A: Extending (And Ending) Support for Windows XP

By J.D. BIERSDORFER

A significant amount of PC's out there are still running Windows XP — about 38 percent as of March 2013, according to the research firm Net Applications, which uses information from computers connected to the Internet. Still, Microsoft has been very open about the fact that it will be retiring Windows XP on April 8, 2014. The Support Lifecycle page for Windows XP even tells visitors to "Buy Windows 8 now!"

A post on one of its official Windows blogs basically states that while PC's running XP will still continue to work after April 8, 2014, they could become targets for malicious software looking to take over newly discovered vulnerabilities in Windows XP. This situation could put users at risk since Microsoft security patches will not be available to plug the holes. The same post also says that antivirus-software companies that still support Windows XP will not be able to fully protect computers running the system. For those inclined to heed the company's persistent warnings, information about upgrading from Windows XP can be found here.

Windows XP stopt ermee?!



zorg anno 1631





datahygiëne

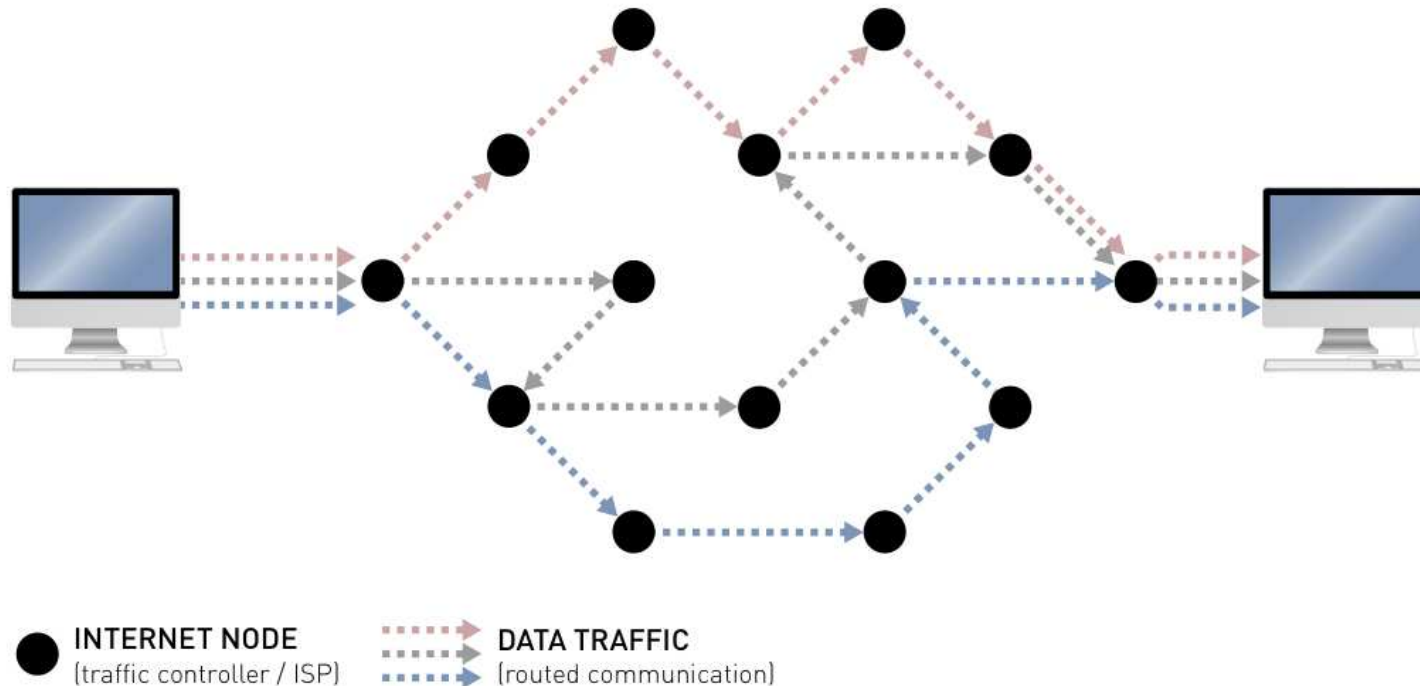
Topje ijsberg

An illustration of an iceberg floating in the ocean. The top of the iceberg is visible above the water line, while the much larger, submerged part is shown below. A small whale is depicted swimming within the submerged portion of the iceberg. The text 'wondere wereld onder water' is written in black across the submerged part of the iceberg.

wondere wereld
onder water

THE INTERNET

A NETWORK OF COMPUTER NETWORKS

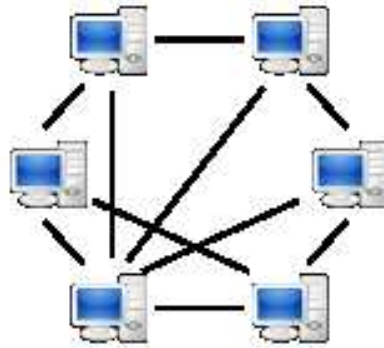


Taal = Internet Protocol (ca. 1974)

talloze applicaties gebaseerd op IP

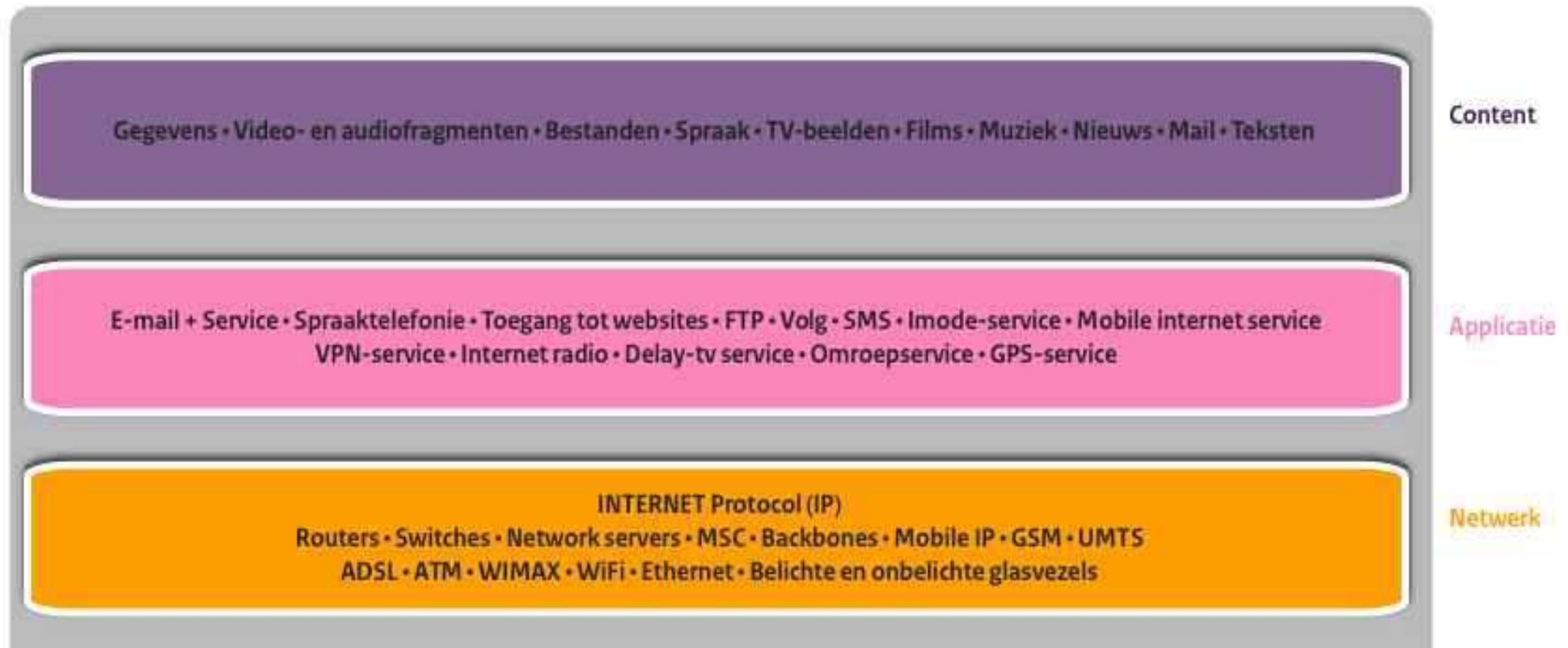


! internet $\Leftrightarrow$ web

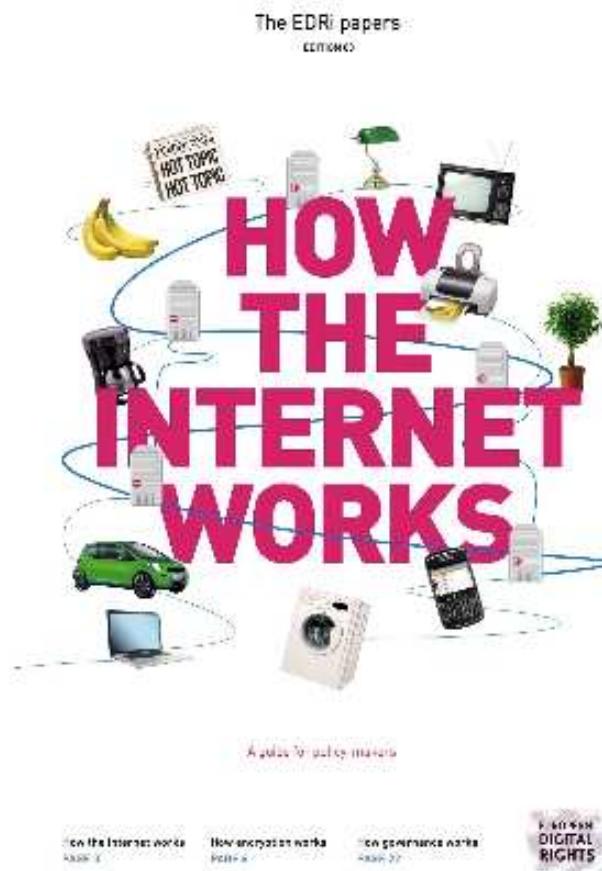


kern succes = openheid/flexibiliteit

Lagenmodel: Content – Applicatie – Netwerk

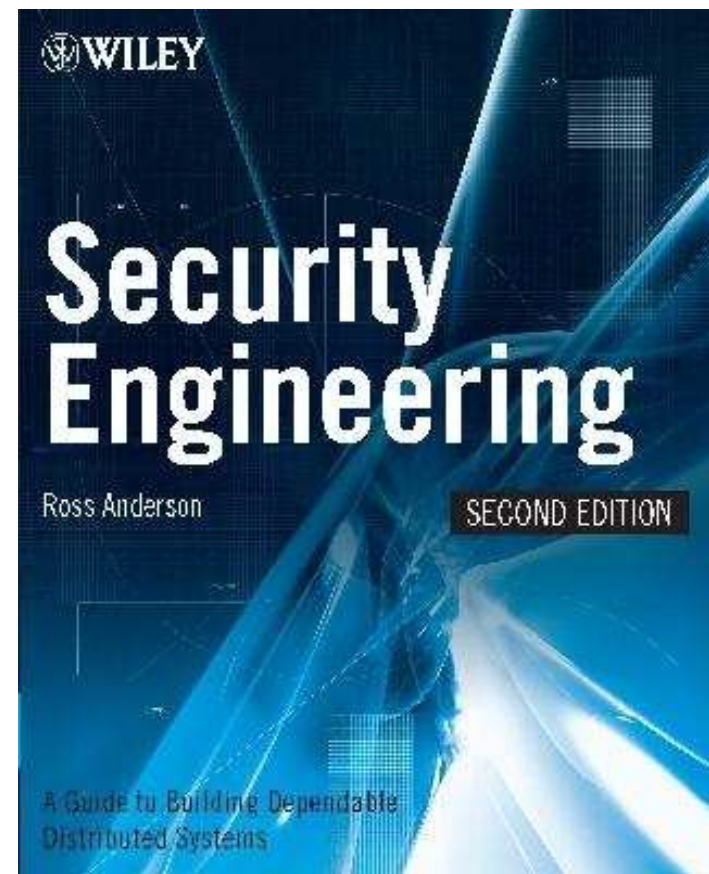


meest urgente security issues in applicatie- en netwerklaag



http://www.edri.org/files/2012EDRiPapers/how_the_internet_works.pdf

bronnen



<http://www.cl.cam.ac.uk/~rja14/book.html>



Internetvrijheid
Toolbox 

<https://www.bof.nl/ons-werk/internetvrijheid-toolbox/>



Twitter: @axelarnbak