Network Security (NetSec)

TECHNISCHE UNIVERSITÄT DARMSTADT

Summer 2015
Chapter 05: Network Level Security
Module 01: Introduction

SECURE MOBILE NETWORKING

CASED

Learning Objectives & Outline

Learn fundamental objectives of network level security mechanisms

- Why network level security: develop an informed opinion
- Scope of protection
- Technologies used for protection on the network level

Outline

(1) Motivation
(2) Recap: the network layer
(3) What can (and what cannot) be protected on network layer
(4) Scope of protection on network level

Chapter 05, Module 01

Motivation

Motivation

SECURE MOBILE NETWORKING

Heise außer kontrolle

Ein Stollen zieht hinaus in die Welt

Stollen, Wind und tapfere Datenfänger - weihnachtlicher geht es nicht mehr

Ein Stollen zieht hinaus in die Welt,
nach Früchten riecht er,
nach Früchten, die so vielen fehlen
und die doch jeder ersehnt,
Ein Stollen zieht hinaus in die Welt,
und ausgetauscht wird er.
Wer immer es hört, der versteht,
leider nicht, um was es geht.

Ach ja, der gute alte Song des Jürgen Marcus ist aktueller denn je, und auch andere weihnachtlich anmutende Texte kommen uns in den Sinn, wenn wir uns über die "Datenpanne" (warum werden solche Datenverluste eigentlich immer als Panne betrachtet, die man mit ein paar schnellen Griffen wieder in den Griff bekommen kann?) der LBB und Karstadt informieren. Wie wir hier lesen können, kommt es zu dieser windigen, verschneiten und stollenbeladenen Zeit schon zu seltsamen Begebenheiten.

Arme, Hunger leidende Kurierfahrer (heißen sie eigentlich David Balfour und Silas?) nehmen, abgemagert und von Früchten und Gewürzen weihnachtlich inspiriert, den Geruch des Christstollens vor ihnen wahr und bedienen sich der magischen Kräfte des weihnachtlichen Festes, die unter anderem die Entfernung von Adressaufklebern ermöglichen, ohne dass das Paket beschädigt wird (allein dafür sollten sie sich www.wir-habens-geschafft.de sichern und dadurch Millionäre werden, denn dieses Wunder ist vielen bis heute nicht gelungen - ich

Thieves Take the Cake

Posted by samzenpus on Monday December 22, @05:39PM
from the **just-eat-it** dept.

Two very hungry German couriers ate a fruit cake destined for a German newspaper and in its place mailed a box of credit card data. The data including names, addresses and card transactions ended up at the Frankfurter Rundschau daily. The mix-up triggered an alarm, and police advised credit card customers with Landesbank Berlin to check their accounts for inconsistencies. Fruitcake must be different in Germany for

DATENKLAU BEI DER LANDESBANK BERLIN

Ein gestohlener Christstollen war schuld!

Der Skandal um die geklauten Kreditkartendaten der Landesbank Berlin (LBB) – eigentlich war es Mundraub! Denn schuld war ein geklauter Christstollen! Den hatten hatten die beiden Kurierfahrer (27, 35) geklaut,

[Sources: slashdot.org, bild.de, heise.de/tp]

Motivation

heise Security

News | Hintergrund | Erste Hilfe | Foren

Security > News > 7-Tage-News > 2012 > KW 17 > VPN-Schlüssel von Finanzdienstleister bei eBay

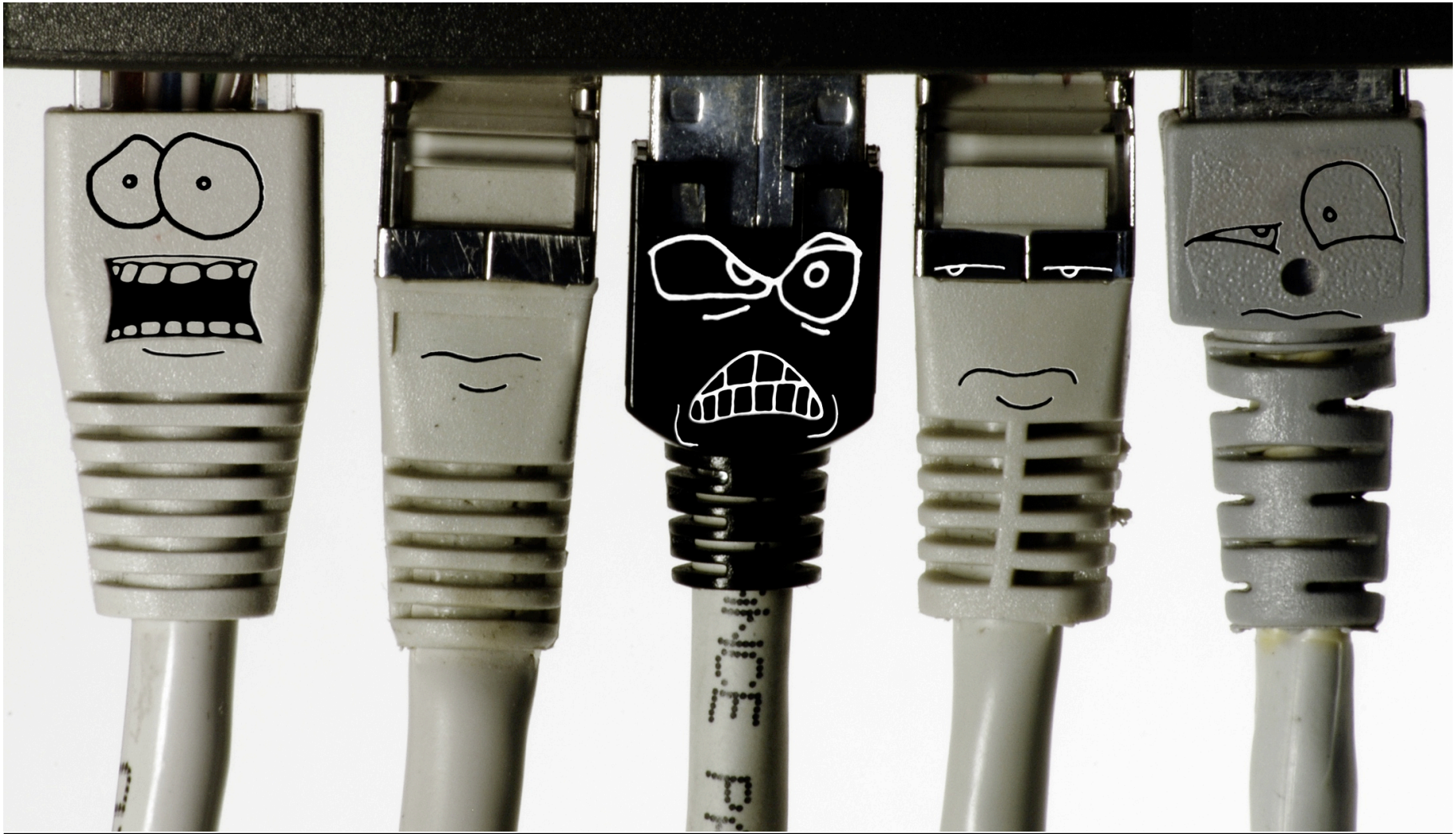
25.04.2012 20:20 « Vorige | Nächste

VPN-Schlüssel von Finanzdienstleister bei eBay aufgetaucht

vorlesen / MP3-Download

In Form kleiner Firewall-Appliances hat der Finanzdienstleistungskonzern Wüstenrot & Württembergische AG praktisch den Schlüssel für sein Unternehmensnetz aus der Hand gegeben, ohne die Schlösser auszuwechseln. Das Intranet der W&W stand Zweitbesitzern der Router offen – etwas Sachkenntnis vorausgesetzt.

Nach dem "Sofortkauf" einiger gebrauchter Firewalls der Marke Juniper Netscreen 5GT bei eBay zum Stückpreis von 19,99 Euro fiel dem Käufer auf, dass die Geräte nicht ordentlich zurückgesetzt worden waren. Sie befanden sich weder in der Default-Konfiguration noch konnte sich der neue Besitzer einloggen. Die Firewall versuchte



Layer 3 Security – Network Layer Security

SEEMOO
SECURE MOBILE NETWORKING

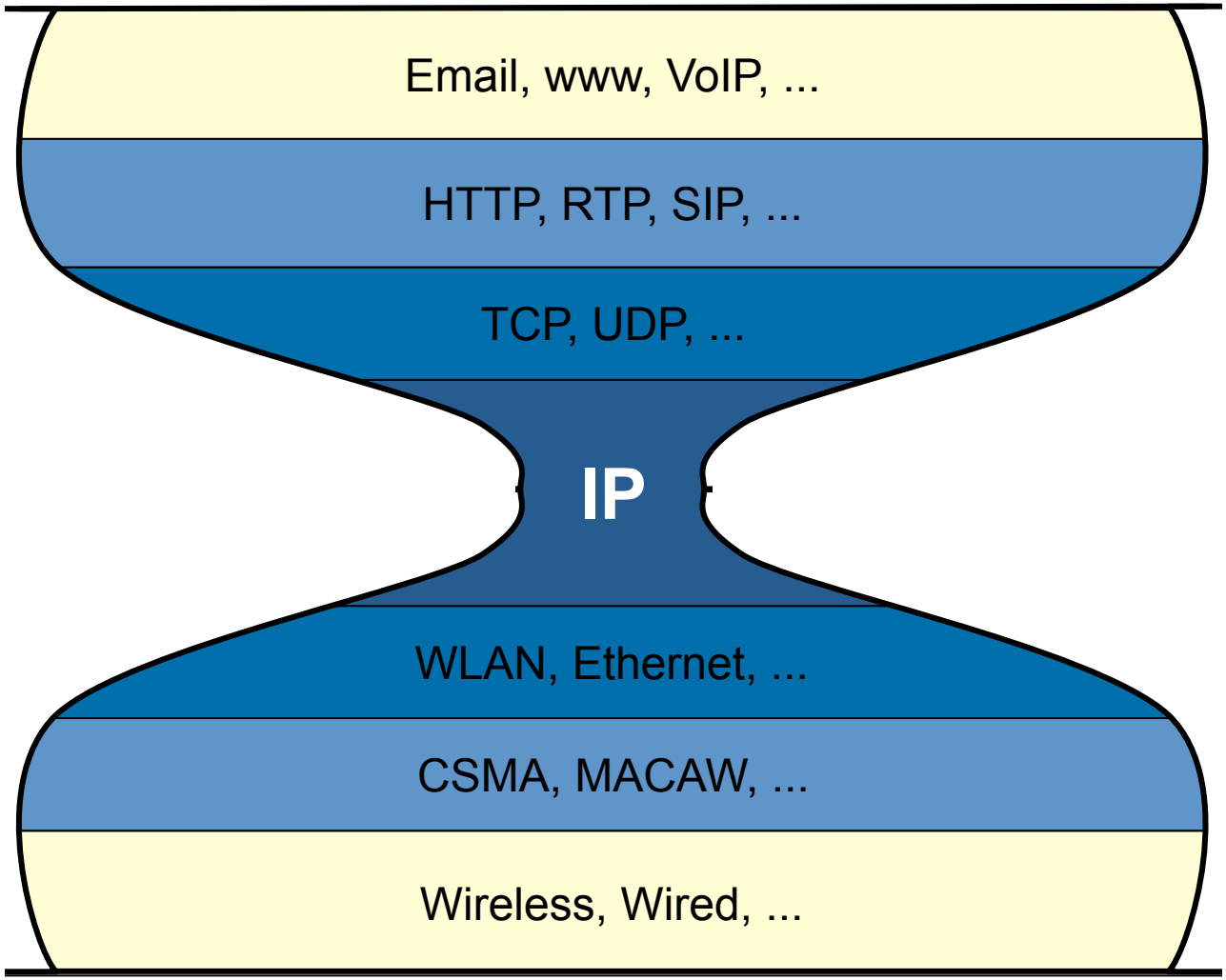
Have you ever set up a „secure network" or a „virtual private network"?

Which technologies did you use?

What were the lessons learned?

Which layer did you choose for your solution?

The Network Layer in the Internet (IPv4)



Technological Motivation for Network Level Security

So far in our lecture: application specific security mechanisms

- e.g. S/MIME, PGP, SSL/TLS/SSH/HTTPS

However there are security concerns that cut across protocol layers (esp. organizational perspective)

- Would like security implemented by the network for all applications

Idea: Don't change applications, just change the OS

- vs. App. Level Security: don't change OS, only change application.
- vs. Transport Level Security: add „security" layer on top of layer 4 (TLS/SSL/SSH) to enable security in apps (that need minor modifications)

What IP offers

IP …

- …provides connectionless and best-effort service
- …basically does not give you any guarantees for the delivery packets

IP datagrams have no inherent security

- IP source address can be spoofed
- Content of IP datagrams can be sniffed
- Content of IP datagrams can be modified
- IP datagrams can be replayed

Securing the Network Layer

Thought experiment:

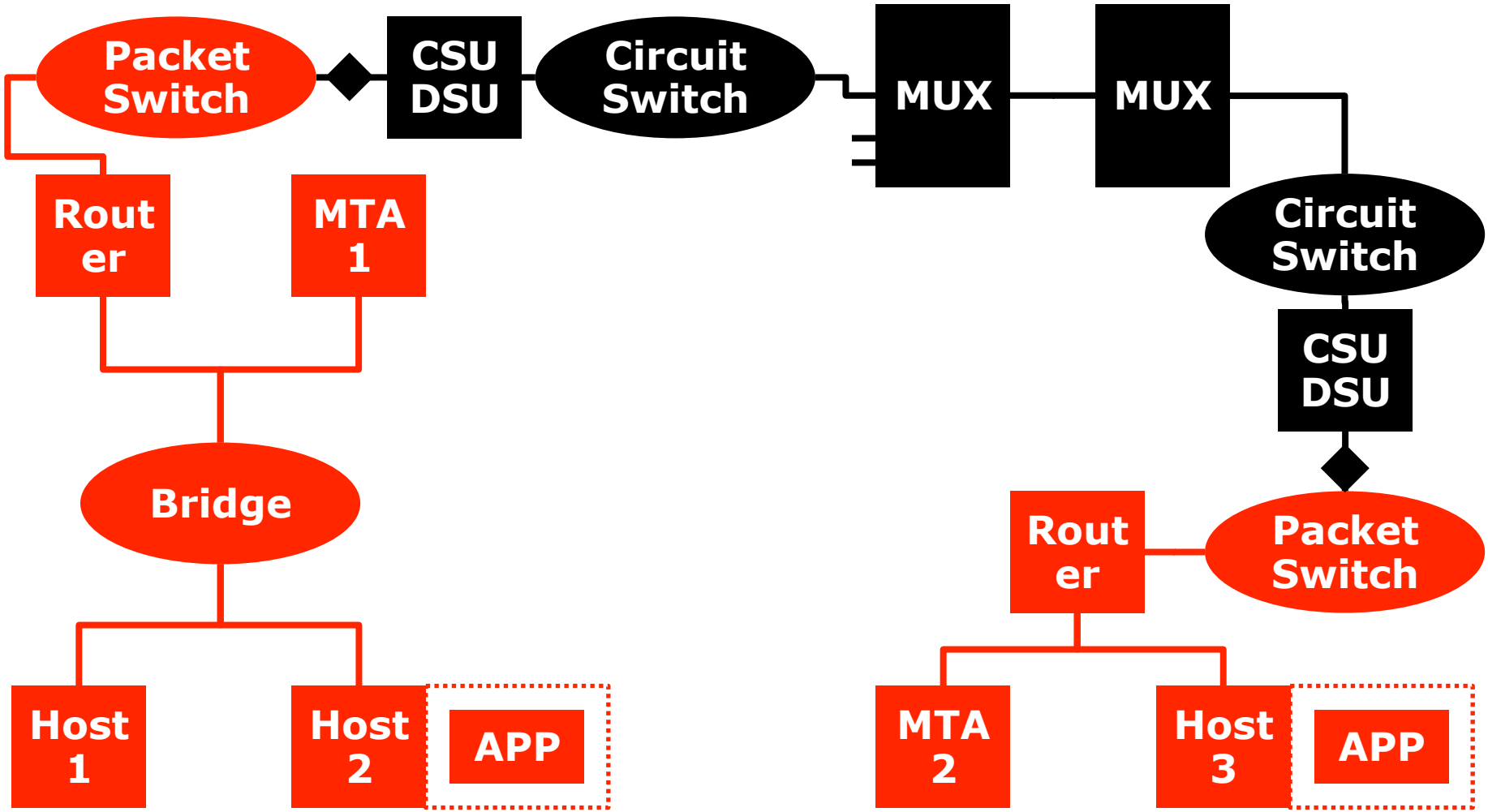
What we could achieve between two network entities:

- Sending entity encrypts the payloads of datagrams.
  - Payload could be: TCP segment, UDP segment, ICMP message, OSPF message etc.
- All data sent from one entity to the other would be hidden:
  - Web pages, Email, P2P file transfers, TCP SYN packets and so on.
- That is „blanket coverage".

But

- API only specifies which IP address to talk to
- All the fancy PKI, names etc. are „useless"
  - no authentication of anything but IP address

L3 - Scope of Protection (Lower Layer 3)



Lower Layer 3 Security

Significant network technology dependence

- Minor protocol suite dependence

Protection

- Data protected in: Black circuits & muxes
- Data unprotected in: Red LANs & bridges, routers & MTAs

Protection granularity: LAN, (sub-)network

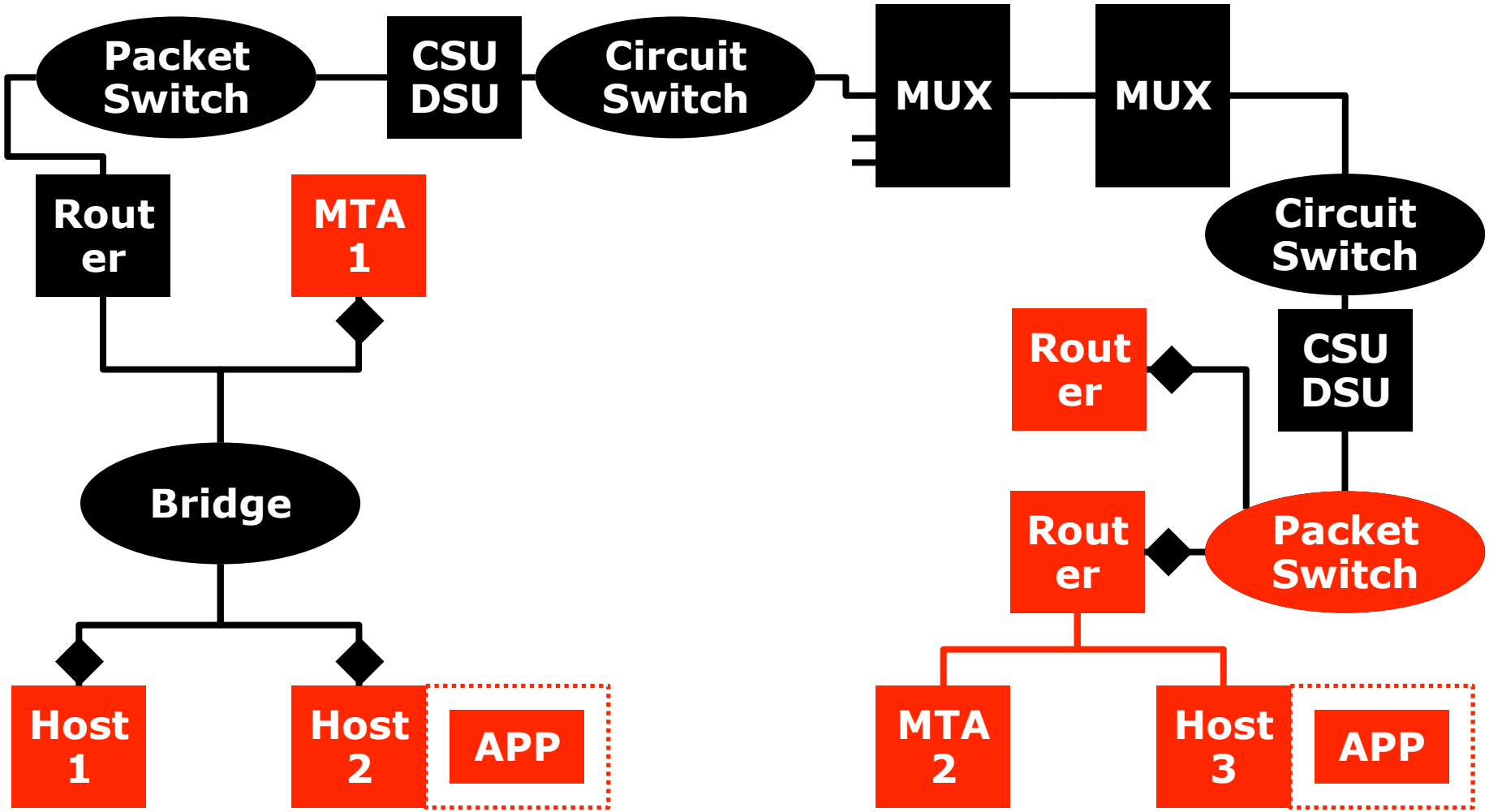
Security services:

- confidentiality (including limited traffic flow confidentiality)
- data origin authentication
- connectionless or connection-oriented integrity (network dependent)
- access control

What is upper and lower Layer 3?

- Taken from OSI world: subnet access(SNAP)/dependend convergence (SNDCP)/independend convergence (SNICP); see also X.25 or CLNP

L3 Scope of Protection (Upper Layer 3 - Internet)



Upper Layer 3 Security

No network technology dependence

- Moderate protocol suite dependence (but IP tunneling mitigates this considerably)

Protection:

- Data protected in: Black circuits & muxes, circuit & packet switches
- Data unprotected in: Red LANs, red MTAs, hosts

Protection granularity: hosts, network

Security services:

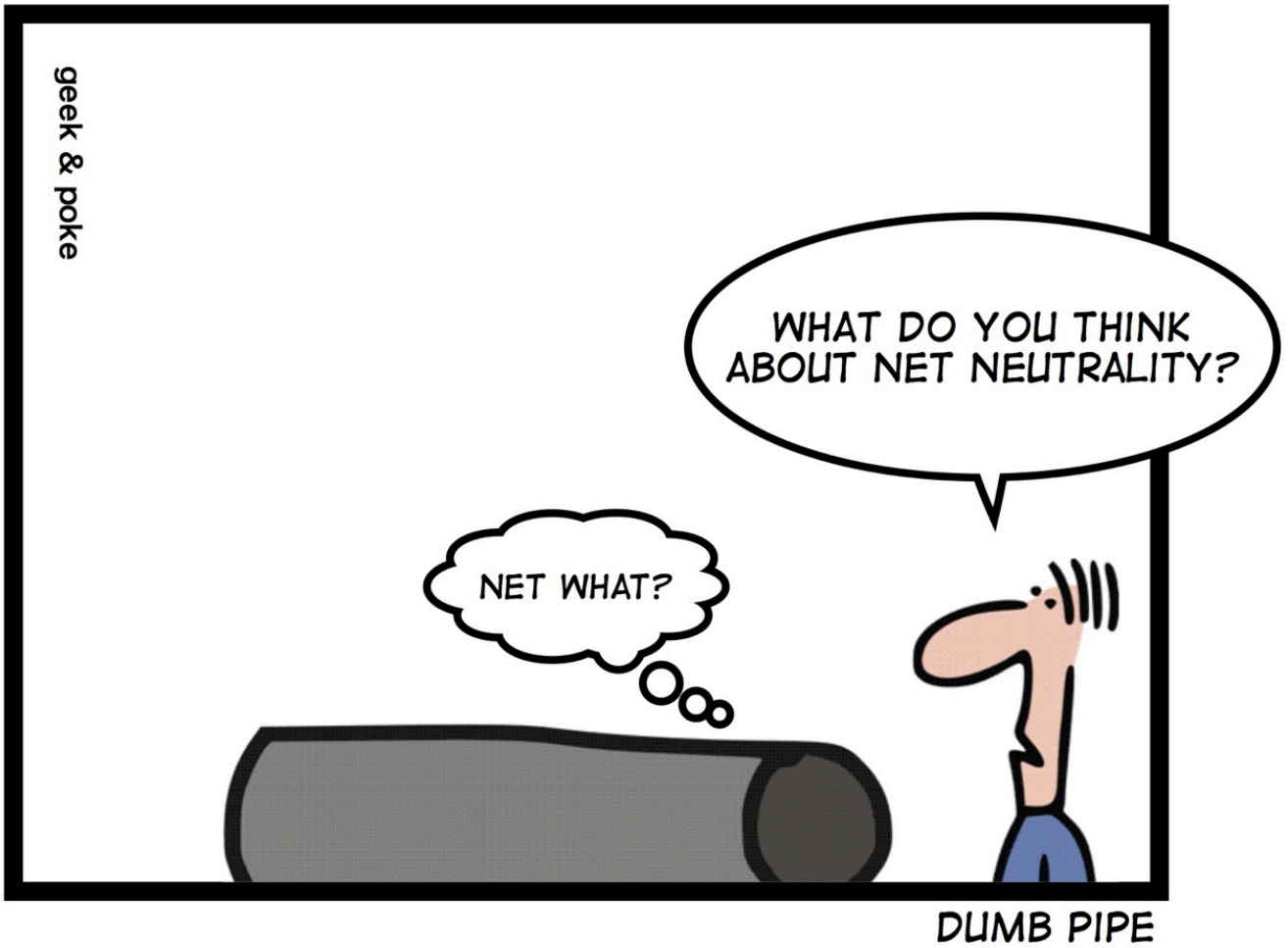
- confidentiality (including limited traffic flow confidentiality)
- data origin authentication
- connectionless & partial sequence integrity
- access control

Summary: Layer 3 Security

Security measures on network layer

- Can offer end-to-end security
  - Sender encrypts/authenticates packets
  - Receiver decrypts/verifies packets
- Does not require changes in every application
  - Security is embedded in network stack/operating system
- Are usually used to set up virtual private networks
  - Secure data exchange via insecure public networks

- Solves rogue packet problem
  - TCP doesn't participate in crypto so attacker can inject bogus packet, no way for TCP to recover
- Easier to do outboard hardware processing (bump in the stack, bump in the wire)


geek & poke
WHAT DO YOU THINK ABOUT NET NEUTRALITY?
NET WHAT?
DUMB PIPE

Acknowledgements

Selected slides of this chapter courtesy of

- Keith Ross, Steven Kent with changes of myself incorporated
- Some other slides courtesy of G. Schäfer (TU Ilmenau) with changes of J. Schmitt (TU Kaiserslautern) and myself incorporated
- Yet some other slides courtesy of R. Perlman, K. Ross, Y. Chen, W. Stallings (L. Brown); changes of myself incorporated
- Some other slides by Marc Werner, SEEMOO

Images taken from:

- www.pixelio.de
- www.renault.fr
- view.stern.de
- www.geekandpoke.com

Recommended Reading

- [KaPeSp2002] Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security – Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002, ISBN: 978-0-13-046019-6

- [Stallings2011] William Stallings, Network Security Essentials, 4th Edition, Prentice Hall, 2011, ISBN: 978-0-136-10805-4

- [Schäfer2003] G. Schäfer. Netzsicherheit - Algorithmische Grundlagen und Protokolle. dpunkt.verlag, 2003.

Copyright Notice