

# Network Security (NetSec)



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

**Summer 2015**

**Chapter 06: Link Level Security**

**Module 01: Intro to Link Level Security**



**Prof. Dr.-Ing. Matthias Hollick**

Technische Universität Darmstadt  
Secure Mobile Networking Lab - SEEMOO  
Department of Computer Science  
Center for Advanced Security Research Darmstadt - CASED

Prof. Dr.-Ing. Matthias Hollick  
[matthias.hollick@seemoo.tu-darmstadt.de](mailto:matthias.hollick@seemoo.tu-darmstadt.de)

Mornewegstr. 32  
D-64293 Darmstadt, Germany  
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921  
<http://seemoo.de> or <http://www.seemoo.tu-darmstadt.de>



# Learning Objectives & Outline



Learn fundamental objectives of link level security mechanisms

- Why link level security
- Scope of Protection

## Outline

- (1) Motivation
- (2) Recap: the link layer
- (3) What can (and what cannot) be protected on link layer

## Chapter 06, Module 01

# Layer 2 – Link Layer Security

Question: What is the role of the link layer?

Question: Which link layer technologies do you know? Do they have security mechanisms?



Source: [www.sxc.hu](http://www.sxc.hu)

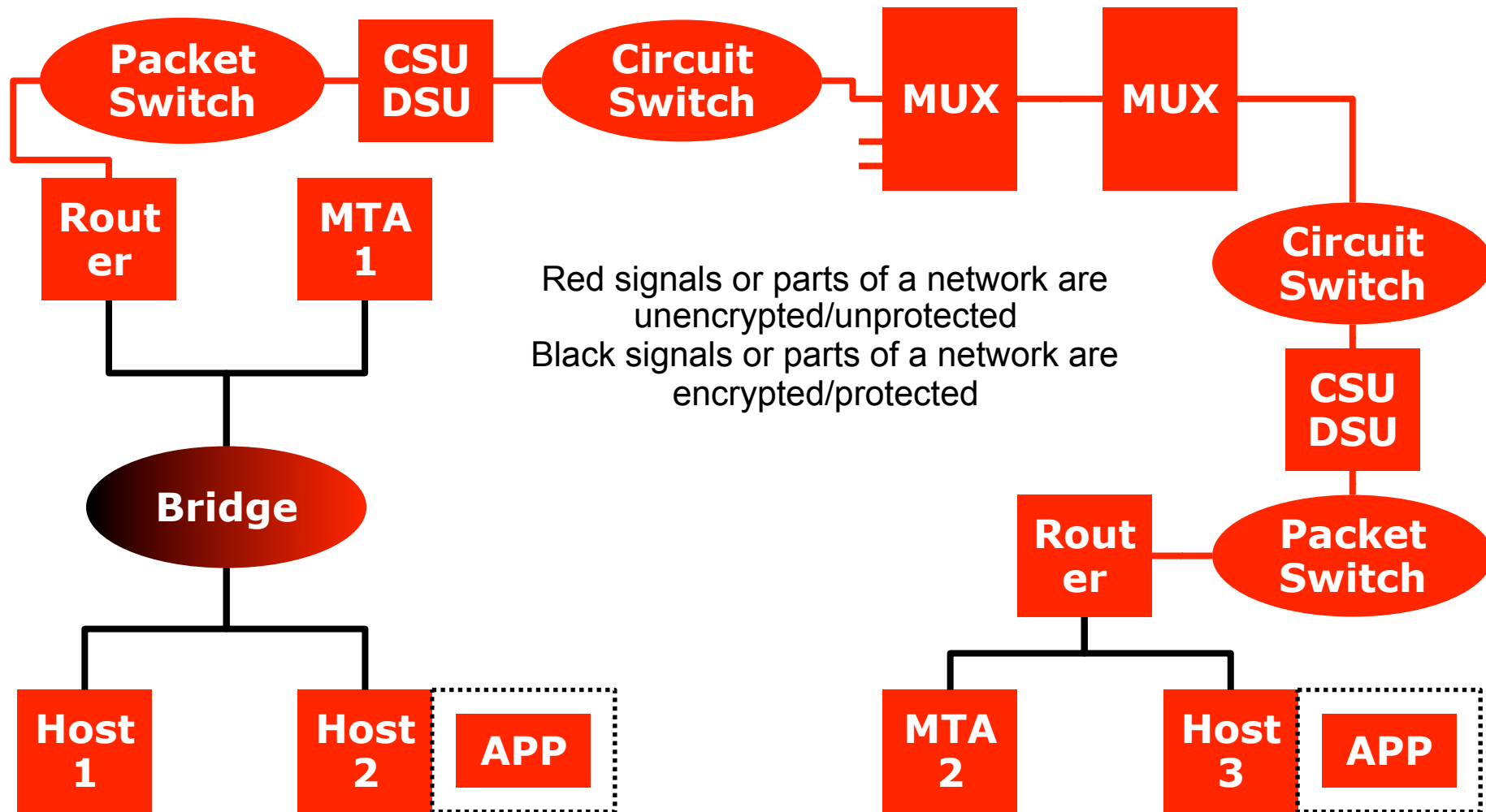
# Data Link Layer – Goals

The goal of the data link layer is to provide reliable, efficient communication between adjacent machines connected by a single communication channel.

Which mechanisms do we typically have to achieve these goals?

Why would we want to secure the link layer?

# L2 - Scope of Protection



# Layer 2 Security

Little network technology dependence (IEEE LANs)

Little protocol suite dependence

Protection

- Red circuits, circuit switches & muxes; black or red LAN segments
- Black or red bridges
- Red packet switches, routers, hosts and MTAs

Protection granularity: individual hosts, LAN segments

Security services:

- confidentiality
- data origin authentication
- connectionless integrity
- access control

# Acks & Recommended Reading



Selected slides of this chapter courtesy of

- 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 S. Kent, R. Perlman, K. Ross, Y. Chen, W. Stallings (L. Brown); changes of myself incorporated

## 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
- [Stallings2015] William Stallings, Network Security Essentials, 4th Edition, Prentice Hall, 2015, ISBN: 978-0-136-10805-4
- [Schäfer2003] G. Schäfer. Netzsicherheit - Algorithmische Grundlagen und Protokolle. dpunkt.verlag, 2003.

---

# Copyright Notice

---

This document has been distributed by the contributing authors as a means to ensure timely dissemination of scholarly and technical work on a non-commercial basis. Copyright and all rights therein are maintained by the authors or by other copyright holders, notwithstanding that they have offered their works here electronically.

It is understood that all persons copying this information will adhere to the terms and constraints invoked by each author's copyright. These works may not be reposted without the explicit permission of the copyright holder.



# Contact



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

**Prof. Dr.-Ing. Matthias Hollick**  
Department of Computer Science

**SEEMOO**  
Mornwegstr. 32  
64293 Darmstadt/Germany  
[matthias.hollick@seemoo.tu-darmstadt.de](mailto:matthias.hollick@seemoo.tu-darmstadt.de)

Phone +49 6151 16-70920  
Fax +49 6151 16-70921  
[www.seemoo.tu-darmstadt.de](http://www.seemoo.tu-darmstadt.de)