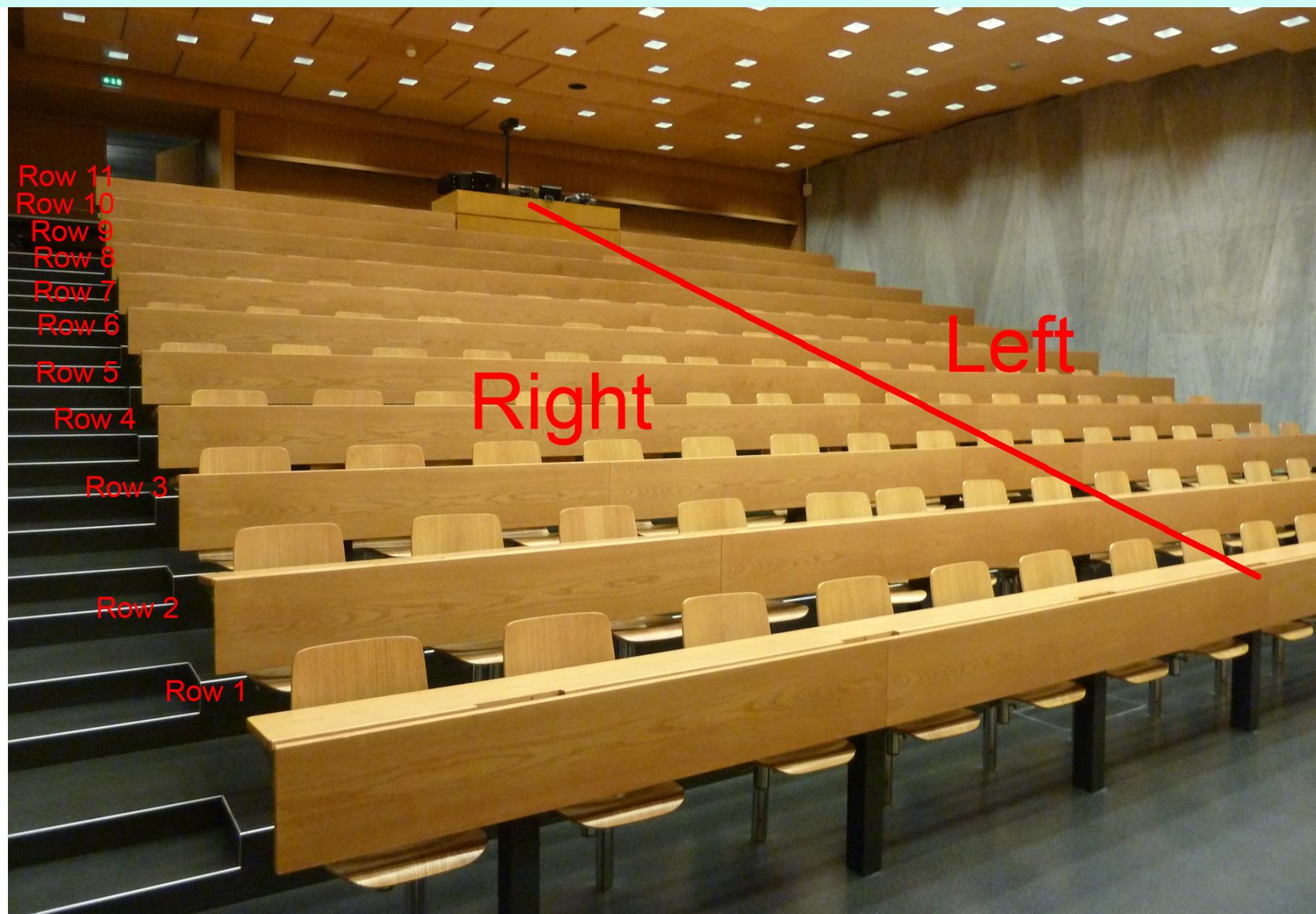


**Seat nr:**  
**4L (3)**  
Ignore  
Left side of row 4



**Remote questions: <https://course.netsec.inf.ethz.ch/questions>**

# Network Security

## Autumn Semester 2020

Introduction and Organization

*15 September 2020*

Prof. Dr. Adrian Perrig  
Dr. Markus Legner  
Dr. Stefan Frei

**ETH** zürich

# Lecture Tickets

In order to attend the lecture in person,  
you must obtain a *lecture ticket* through GitLab

The screenshot shows a GitLab issue page for the NetSec Course. The title of the issue is "Lecture registration 2020-09-15". The description includes instructions for requesting a seat by giving a thumbs up, a priority list for last names (Imnopqrstuvwxyz), and a notification email. A large red arrow points from the thumbs up button at the bottom left to the email response on the right.

ETH zürich DINFK GitLab Projects Groups More + Q D 1 1 ?

PRV-PERRIG > 🚨 NetSec Course > 📱 NetSec 2020 Student Issues > Issues > #8

Open Opened 6 days ago by 🤖 NetSec Course Close issue New issue

## Lecture registration 2020-09-15

Participate in this issue (e.g., by giving a thumbs up below) to request a seat for the NetSec lecture of 2020-09-15.

This week students with last names starting with one of the following letters get priority:  
**Imnopqrstuvwxyz.**

You will be notified via email on 2020-09-14 at 07:00:00 about your assigned seat.

To upload designs, you'll need to enable LFS. [More information](#)

54 0

Oldest first Show all activity

[NetSec-seats] Seat 2L (1) assigned for 2020-08-18

NetSec Course <[networksecurity@lists.inf.ethz.ch](mailto:networksecurity@lists.inf.ethz.ch)>  
Mon 8/17, 7:00 AM  
De Vaere Piet

Dear Piet

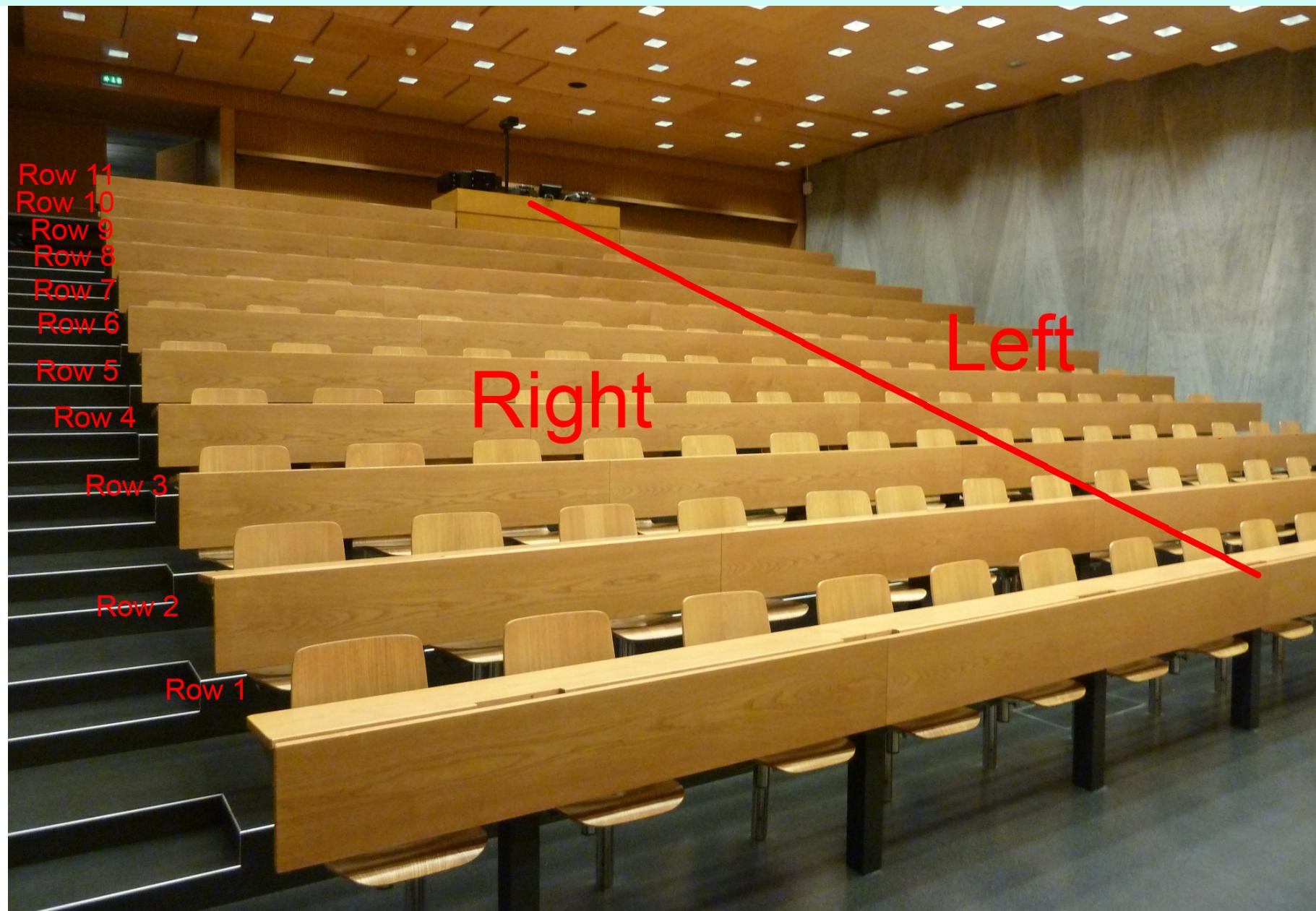
You have been assigned seat 2L (1) for the NetSec lecture of 2020-08-18.

Kind regards  
The NetSec team

# COVID-19 Measures

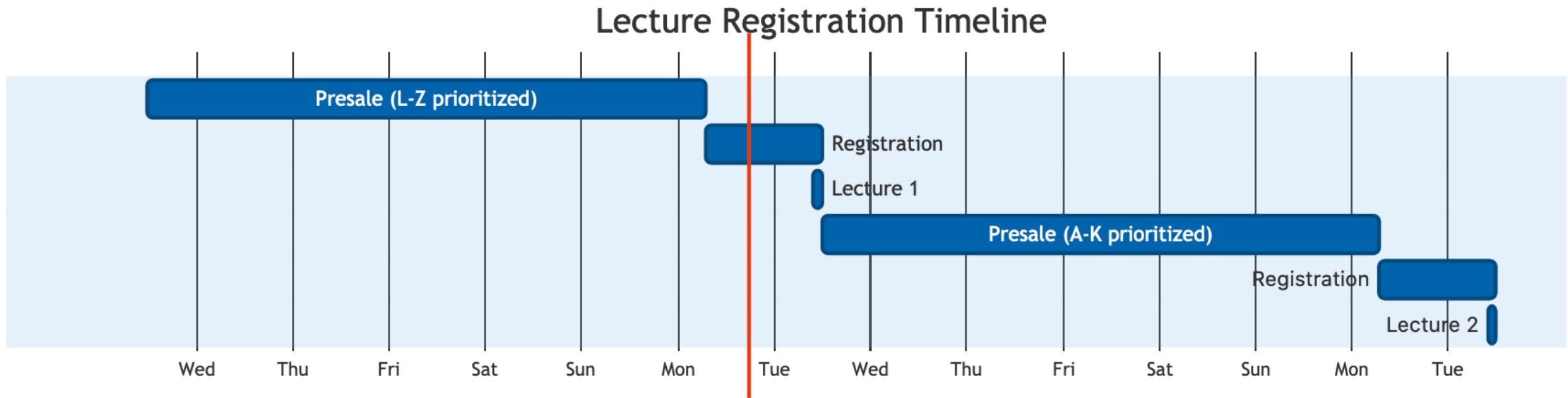
- Follow the general safety guidelines.
- **Always** wear a face mask over mouth and nose.
- **Do *not* attend the lecture if you have illness symptoms!**

**Seat nr:**  
**4L (3)**  
Ignore  
Left side of row 4



# Lecture Tickets

Alternating prioritization ensures that you can visit at least every other lecture.



More information on GitLab (see later)

# Network Security in the News

Hackers attacking US and European energy firms could sabotage power grids



The Register®  
Biting the hand that feeds IT

[DATA CENTRE](#) [SOFTWARE](#) [SECURITY](#) [DEVOPS](#) [BUSINESS](#) [PERSONAL TECH](#) [SCIENCE](#) [EMERGENT TECH](#) [BOOTNOTES](#) [VENDOR VOICE](#) [LOG IN](#)

{\* SECURITY \*}

## There are DDoS attacks, then there's this 809 million packet-per-second tsunami Akamai says it just caught

Bank on the receiving end of massive 418Gbps traffic barrage

Thu 25 Jun 2020 // 10:03 UTC

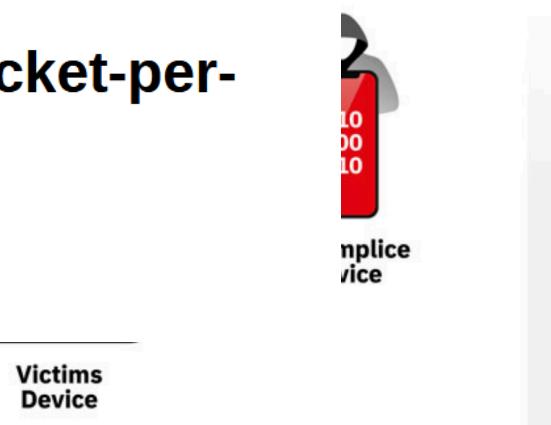
50 GOT TIPS?



Symantec reports the hacking group appears to be in information-gathering mode, but warns this could pre-empt an attempt at sabotage. Photograph: Gareth Fuller/PA

A hacking campaign is targeting the energy sector in [Europe](#) and the US to potentially sabotage national power grids, a cybersecurity firm has warned.

The group, dubbed "Dragonfly" by researchers at Symantec, has been in operation since at least 2011 but went dark in 2014 [after it was first exposed](#), secretly



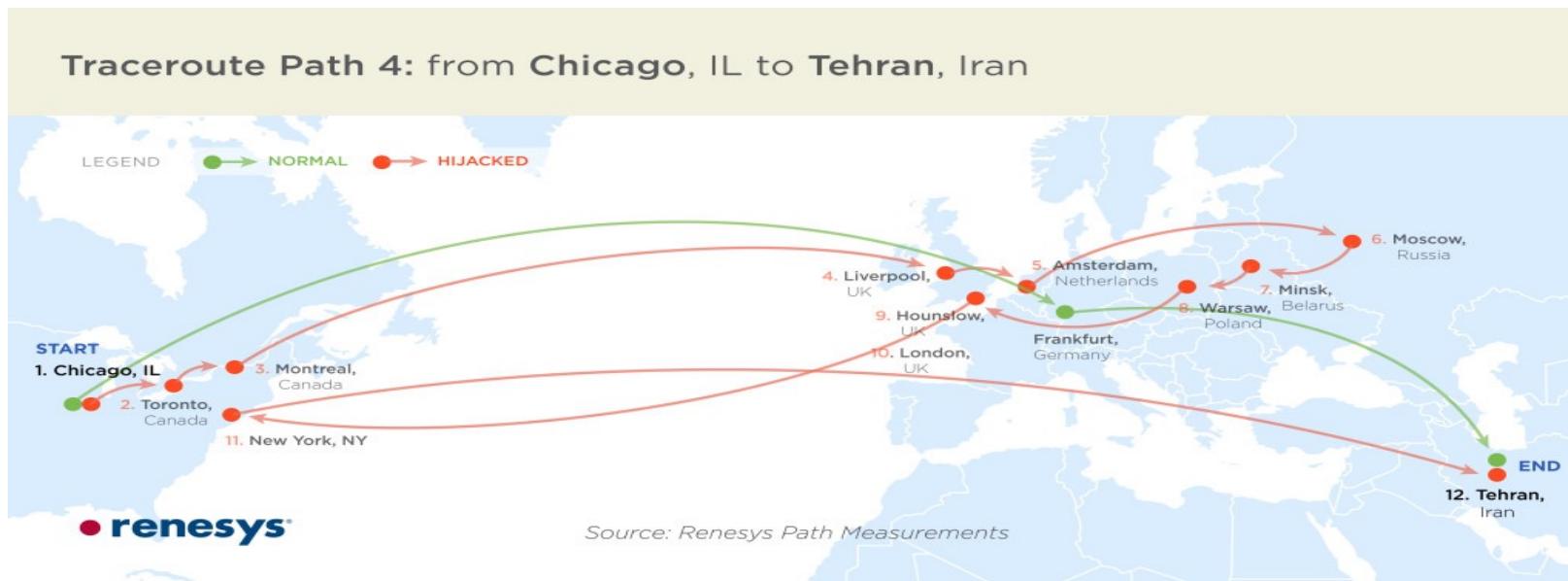
Victims  
Device

Cybersecurity researchers today revealed the existence of a new and previously undetected critical vulnerability in SIM cards that could allow remote attackers to compromise targeted mobile phones and spy on victims just by sending an SMS.

Dubbed "SimJacker," the vulnerability resides in a particular piece of software, called the S@T

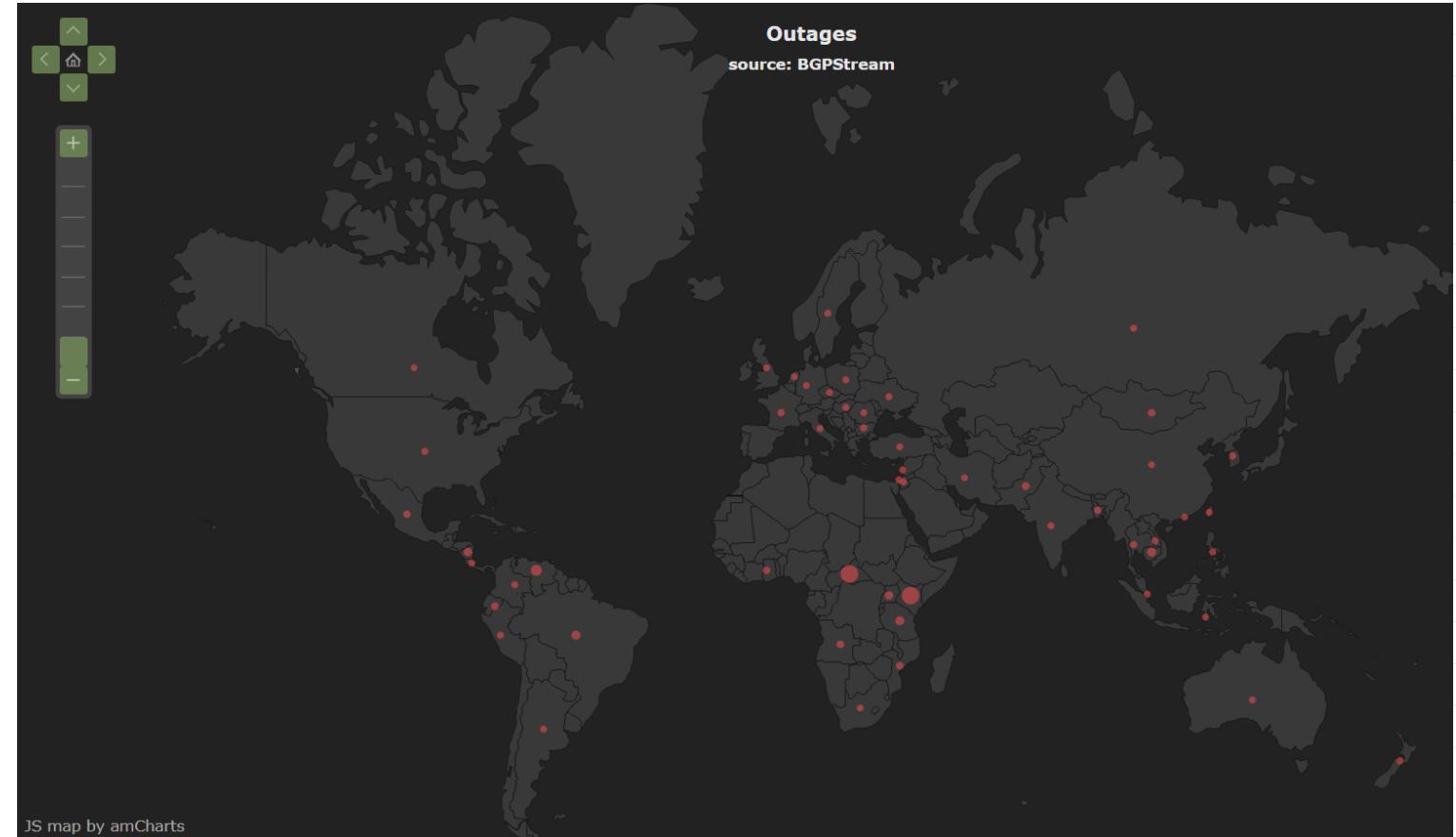
Remote questions: <https://course.netsec.inf.ethz.ch/questions>

# Daily Internet Attack: BGP Prefix Hijacking



# Attack Monitor: bgpstream.com

Event type	Country	ASN	Start time (UTC)	End time (UTC)
Possible Hijack		Expected Origin AS: COGENT-174, US (AS 174) Detected Origin AS: EAGLENET, LB (AS 60372)	2020-09-14 20:42:41	
Possible Hijack		Expected Origin AS: COGENT-174, US (AS 174) Detected Origin AS: EAGLENET, LB (AS 60372)	2020-09-14 20:42:41	
Possible Hijack		Expected Origin AS: IPMEN, GB (AS 209372) Detected Origin AS: RU-FIXED-KRSK, RU (AS 57129)	2020-09-14 19:47:29	
Outage	VALLEY-COMMUNICATIONS, US	(AS 394972)	2020-09-14 19:41:00	2020-09-14 19:44:00
Possible Hijack		Expected Origin AS: SIGNET-AS, NL (AS 28878) Detected Origin AS: COLT Technology Services Group, SE (AS 15404)	2020-09-14 19:34:52	
Possible Hijack		Expected Origin AS: SIGNET-AS, NL (AS 28878) Detected Origin AS: COLT Technology Services Group, SE (AS 15404)	2020-09-14 19:34:52	
Outage	INFOSTROY-AS INFOSTROY AS, RU	(AS 208397)	2020-09-14 16:48:00	2020-09-14 16:55:00
Outage	INFOSTROY-AS INFOSTROY AS, RU	(AS 208397)	2020-09-14 16:33:00	2020-09-14 16:36:00
Possible Hijack		Expected Origin AS: JOSE MARIA DELFINO(TELMIIX), PY (AS 269763) Detected Origin AS: (AS 269764)	2020-09-14 16:22:20	
Possible Hijack		Expected Origin AS: GROUPNET, IQ (AS 209699) Detected Origin AS: ALSARD, IQ (AS 39216)	2020-09-14 15:29:59	
Possible Hijack		Expected Origin AS: FORCEPOINT-CLOUD-AS, EU (AS 44444) Detected Origin AS: ASN-ORANGE-ROMANIA, RO (AS 8953)	2020-09-14 15:07:56	
Possible Hijack		Expected Origin AS: SMPHI-AS-AP SM Prime Holdings, Inc., PH (AS 58884) Detected Origin AS: SMIC-AS-AP SM Investments Corporation, PH (AS 141016)	2020-09-14 14:56:46	
Outage	Global Conect Ltda, BR	(AS 262735)	2020-09-14 13:56:00	
Possible Hijack		Expected Origin AS: ASSKYNET, LB (AS 48418) Detected Origin AS: Beirut-Lebanon, LB (AS 9051)	2020-09-14 13:50:41	
Possible Hijack		Expected Origin AS: ALTIMA-TELECOM, CA (AS 22423) Detected Origin AS: SPRINTLINK, US (AS 1239)	2020-09-14 12:11:04	
Possible Hijack		Expected Origin AS: ALEXHOST_SRL, MD (AS 207636) Detected Origin AS: SPRINTLINK, US (AS 1239)	2020-09-14 12:11:04	
Outage	INFOSTROY-AS INFOSTROY AS, RU	(AS 208397)	2020-09-14 12:04:00	2020-09-14 12:10:00
Outage	COOPERATIVAS DE CALAMUCHITA - CONSORCIO DE COOPERACION, AR	(AS 263230)	2020-09-14 11:55:00	2020-09-14 11:58:00
Outage	INFOSTROY-AS INFOSTROY AS, RU	(AS 208397)	2020-09-14 11:54:00	2020-09-14 11:58:00
Outage	KI	N/A	2020-09-14 09:42:00	
Outage	BENCHMARK-AS-IN Benchmark Infotech Services Pvt.Ltd., IN	(AS 58966)	2020-09-14 09:34:00	2020-09-14 09:37:00
Outage	KINGS-AS-ID Kings Network Indonesia, PT, ID	(AS 45725)	2020-09-14 06:51:00	
Possible Hijack		Expected Origin AS: ESINNET Shenzhen ESIN Technology Co., Ltd, CN (AS 59072) Detected Origin AS: ULAN-NETWORK-LIMITED Ulan Network Limited, HK (AS 134196)	2020-09-14 01:40:00	
Outage	COFRACATAL-001, US	(AS 26073)	2020-09-14 01:24:00	2020-09-14 01:31:00



# Network Components are Also Vulnerable

## Hackers Infect Over 100k Routers With Crypto Mining Malware

August 02, 2018 • Mohit Kumar

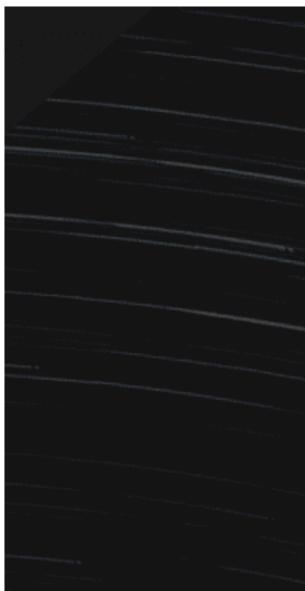


Security researchers have discovered thousands of unpatched MikroTik routers connected to them.

In all, the malware campaigns have targeted hardware provider Mikrotik across

## Thousands of MikroTik Routers Infected With Malware On Network Traffic

September 03, 2018 • Swati Khandelwal



Last month we reported about the discovery of thousands of unpatched MikroTik routers using a previously unknown exploit.

Now Chinese security researchers have found a new vulnerability in MikroTik routers, which can be exploited maliciously, allowing attackers to gain access to the routers' configuration files.

Cybersecurity researchers have found a new vulnerability in MikroTik routers, which can be exploited maliciously, allowing attackers to gain access to the routers' configuration files.

TELECOMS TAKE NOTE —

## Attackers are trying to exploit a high-severity zero-day in Cisco gear

Exploits can exhaust memory in hardware used by telecoms and cloud providers.

DAN GOODIN - 8/31/2020, 9:59 PM

## Some MikroTik Routers Still Infected With Malware

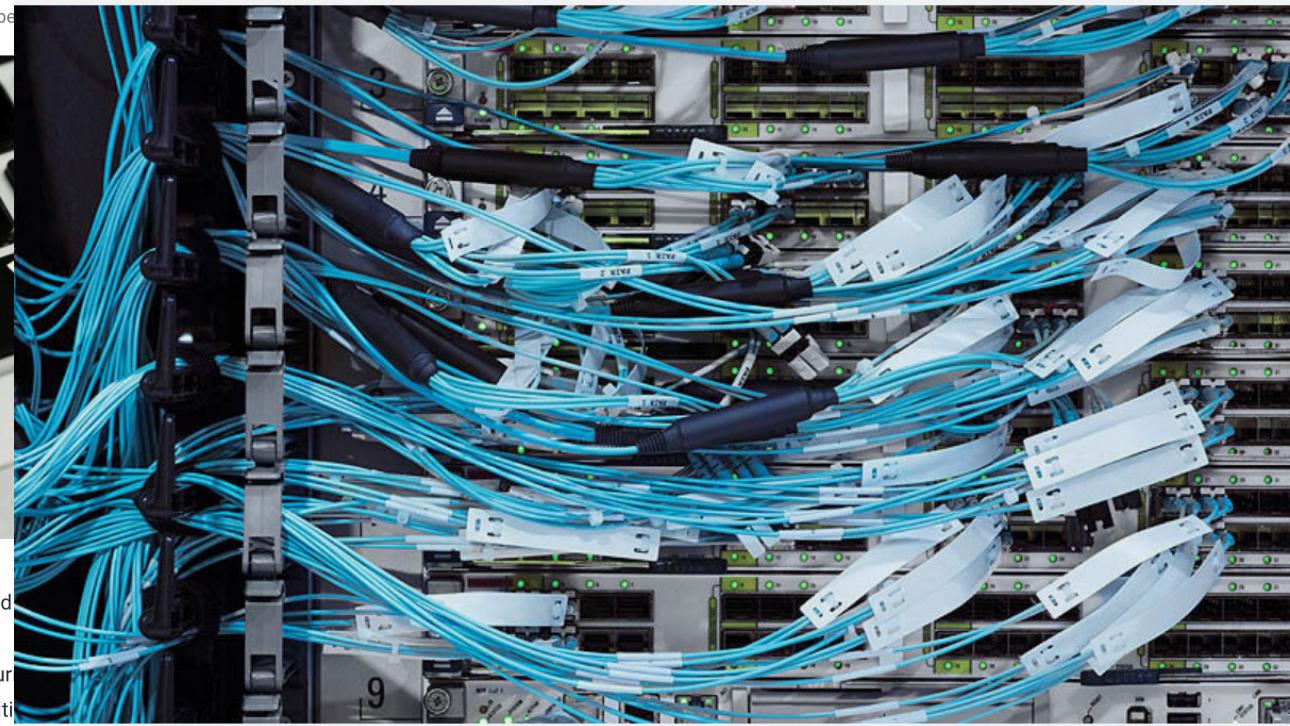
September 03, 2018 • Swati Khandelwal



What could

Cybersecu

vulnerabilit



—that involve insecure storage of credentials, potentially affecting every user and system on that

# Example: Ethereum Wallet Heist

# About This Course

- The course will cover topics spanning four broad themes:
  - Network **defense mechanisms** such as secure routing protocols, TLS, anonymous communication systems, network intrusion detection systems, and public-key infrastructures;
  - Network **attacks** such as denial of service (DoS) and distributed denial-of-service (DDoS) attacks;
  - Attack **analysis and inference** topics such as network forensics and attack economics;
  - Secure **next-generation network architectures**.
- We will assume knowledge of the “Computer Networks” course taught in the spring semester (<https://ndal.ethz.ch/courses/networks.html>)
  - “Networking Refresher” in exercise session this week
  - More pointers during the course
  - No specific questions in exam, but may be required to answer other questions

# Draft Syllabus

AP	Course introduction, crypto refresher
AP	PKI systems
KP	TLS
KP	TLS
ML	VPNs, IPsec, Wireguard
ML	Anonymous-communication systems
ML	BGP security, BGPsec, best practices
ML	(D)DoS attacks and current defense mechanisms
SF	DNS security and privacy
SF	Firewalls, IDS, evasion and limitations
SF	Cybersecurity in practice / legal aspects
AP	Probabilistic traffic-monitoring techniques
AP	Next-generation Internet (SCION)
AP	Next-generation PKIs + DRKey

# Learning Objectives

- You are familiar with fundamental **network-security concepts**.
- You can **assess current threats** that Internet services and networked devices face and can evaluate appropriate countermeasures.
- You can **identify and assess known vulnerabilities** in a software system that is connected to the Internet (through analysis and penetration testing tools).
- You have an in-depth understanding of a range of important **security technologies**.
- And: You develop some **intuition** and reasonable **paranoia** in your work with ICT.

# Lecturers



**Prof. Dr. Adrian Perrig**, Twitter @adrianperrig

- Since 2013, Professor of Computer Science, ETH Zürich
- 2002-2012: Professor at Carnegie Mellon University
- Core focus: network and systems security, secure communication architectures



**Dr. Stefan Frei**, Twitter @stefan\_frei

- Senior Security Principal, Accenture Cyber Defense
- PhD ETH Zurich
- Formerly VP Research NSS Labs, Austin/TX, USA, Research Director Secunia
- Penetration Tester/Researcher ISS X-Force (now part of IBM)



**Dr. Markus Legner**,

- Postdoctoral Researcher, Network Security Group
- PhD ETH Zurich (in theoretical physics)
- Working on further improving data-plane security and quality of service for SCION



**Prof. Dr. Kenny Paterson**, Twitter @kennyog

- Since 2019, Professor of Computer Science, ETH Zürich
- Until 2019: Professor at University of London
- Core focus: applied cryptography, many contributions to TLS

# Lecture and Exercise Sessions

## Lecture:

**Tue 10:00-12:00, CHN C 14**

- Key security concepts, theory, technologies, case studies
- Schedule and topics at <https://www.netsec.ethz.ch/courses/netsec-2020/>

## Exercise session and guest talks:

**Thu 16:00-18:00, HG F 1**

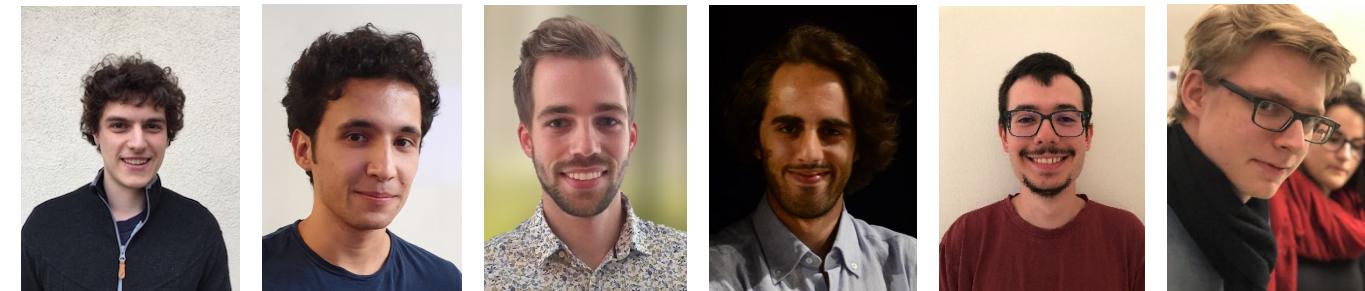
- “Attack show cases”, discussion of assignments, guest talks

## Teaching assistants

- Piet De Vaere, Head TA
- Giacomo Giuliari, Exercise TA
- Simon Scherrer, Project TA

## Student assistants

- Matteo Scarlata
- Marc-Philippe Bartholomä
- Ben Fiedler, DtF project



# Exercise Sessions

- Will take place on Thursday 16:15–18:00 in HG F 1
- Sessions will consist of:
  - 1 hour discussion of last exercise sheet
  - 1 hour of one of the following:
    - Guest lecture
    - Project discussion
    - Question hour
- First exercise session is this Thursday (17.09.2020)
  - By exception this exercise session will contain a “Networking Refresher” lecture

## Guest Lectures

**We will again have exiting guest lectures this year**

- Nico Schottelius, **Ungleich**, “Security Aspects of IPv6”
- Maxim Salomon, **Google**, “Security vulnerabilities of modern Wireless LAN Systems”
- Rayhaan Jaufeerally, **AS210036**, “An exploration of real-world network security”
- Candid Wüest, **Acronis**, “Malware Analysis and Prevention”
- Patrick Schmid, **RedGuard**, “Top X Ways to get Domain Admin”
- David Mc Laughlin, **ETH Zürich**, “Email spam prevention at ETH”

**Remote questions: <https://course.netsec.inf.ethz.ch/questions>**

## Course Webpage

The course's webpage is at:

**<https://netsec.ethz.ch/courses/netsec-2020/>**

Course materials (slides, exercises, ...) will be distributed through a GitLab repository linked to on this page. Course registration is required for access.

Lecture recordings will be distributed through the ETH video portal.

Remote questions: <https://course.netsec.inf.ethz.ch/questions>

# GitLab

The screenshot shows the D-INFK GitLab interface. The top navigation bar includes links for ETH zürich, D INFK GitLab, Projects, Groups, More, a search bar, and various user icons. On the left, a sidebar for the 'NetSec Course' group lists Subgroup overview, Details (selected), Activity, Issues (2), Merge Requests (0), and Members. The main content area displays the 'NetSec Course' group details, which is a Network Security MSc course. It features a cartoon character icon, the group name 'NetSec Course' with a lock icon, and Group ID 6769. Below this, there are sections for Subgroups and projects, Shared projects, and Archived projects. A search bar and filters for 'Last created' are also present. Two projects are listed: 'NetSec 2020 Student Resources' (Reporter, 2 stars, 4 hours ago) and 'NetSec 2020 Student Issues' (Guest, 2 stars, 1 week ago).

We use the D-INFK GitLab instance: <https://gitlab.inf.ethz.ch>

# GitLab Resources

The screenshot shows a GitLab project page for 'NetSec 2020 Student Resources'. The sidebar on the left includes links for Project overview, Details, Activity, Releases, Repository, Operations, Analytics, and Members. The main content area displays the project details, including a summary of 15 commits, 1 branch, 0 tags, 13.9 MB files, and 13.9 MB storage. It also shows a commit from Piet De Vaere, a README file, and a table of files with their last commit and update times. A 'Network Security (NetSec) 2020 User Manual' section is present at the bottom.

NetSec 2020 Student Resources

Project ID: 10911 | [Leave project](#)

15 Commits 1 Branch 0 Tags 13.9 MB Files 13.9 MB Storage

Student resources for the Fall 2020 Network Security Course

master netsec-2020-resources

removed .dir placeholder  
Piet De Vaere authored 7 minutes ago

b8660c93

README No license. All rights reserved

Name	Last commit	Last update
exercises	removed .dir placeholder	7 minutes ago
lectures	created directories for lecture slides and exercises	2 weeks ago
old_exams	added old exams	2 weeks ago
README.md	swapped odd and even name based prioritization for lecture tick...	1 day ago
chn_c_14.annotated.jpg	actually adding new smaller picture	2 weeks ago

README.md

### Network Security (NetSec) 2020 User Manual

Welcome to the NetSec course! For this course, GitLab will serve as the main point of (online) interaction between students and the course team. Concretely, using this GitLab you will

- receive lecture materials such as slides, exercises, and old exams;

Slides  
Exercises  
Old Exams  
Project Descriptions  
...

# GitLab Issues

We will use the GitLab issue tracker extensively in this course:

- Lecture registration
- Questions about lecture, exercises, projects
- Administrative questions
- Handing in exercises
- ...

PRV-PERRIG > 🛡 NetSec Course > NetSec 2019 Students > Issues > #75

**Closed** Opened 7 months ago by [redacted] Report abuse

### Difference between EPIC Level 2 and PISKES

I don't really understand what the difference between EPIC and PISKES is. EPIC Level 2 achieves source authentication using DRKey (Slide 20) and PISKES, according to slide 24, does the same. It seems like they are just the same thing? Or what makes them different?

To upload designs, you'll need to enable LFS. [More information](#)

0 likes 0 dislikes Oldest first Show all activity

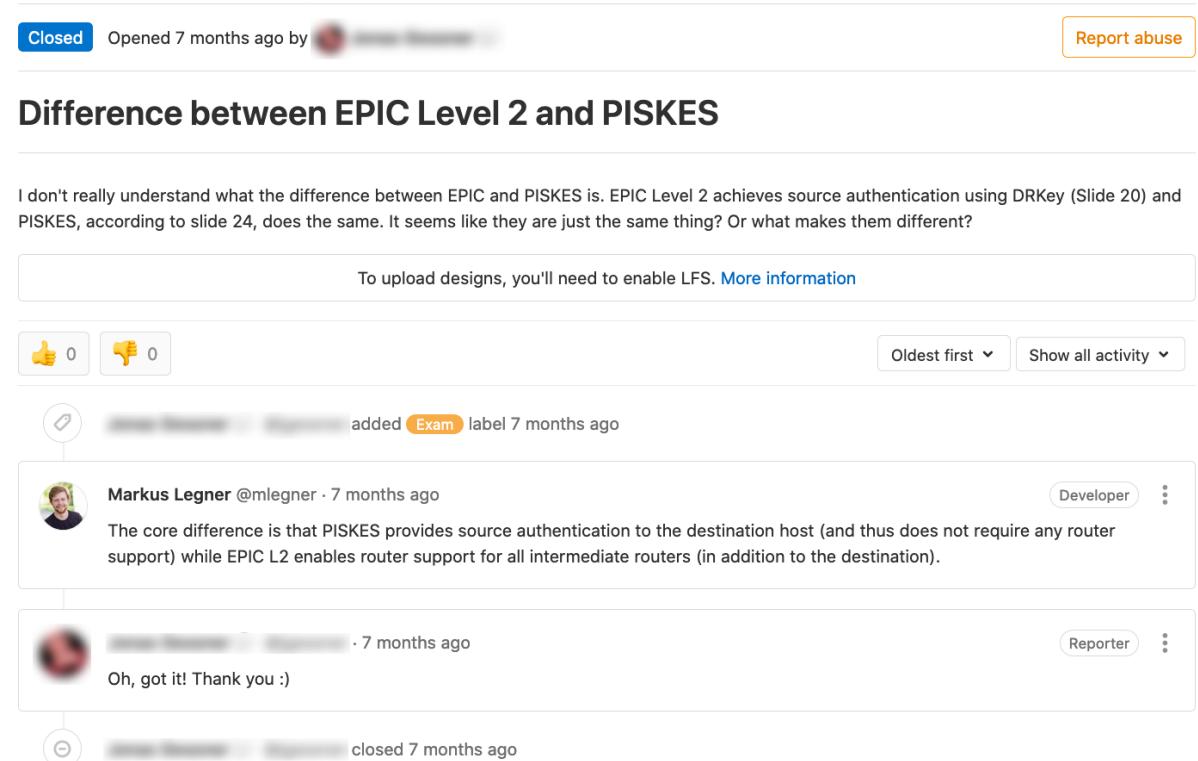
added Exam label 7 months ago

Markus Legner @mlegner - 7 months ago Developer

The core difference is that PISKES provides source authentication to the destination host (and thus does not require any router support) while EPIC L2 enables router support for all intermediate routers (in addition to the destination).

Oh, got it! Thank you :) Reporter

closed 7 months ago



# Private questions through GitLab

PRV-PERRIG > 🇨🇭 NetSec Course > 🏃 NetSec 2020 Student Issues > Issues > New

## New Issue

Title

Super private question

Description

Write Preview



I do not want other students to see this

Markdown and [quick actions](#) are supported

Attach a file

This issue is confidential and should only be visible to team members with at least Reporter access.

Submit issue

Cancel

Remote questions: <https://course.netsec.inf.ethz.ch/questions>

# Handing in Exercises through GitLab

PRV-PERRIG > 🧑 NetSec Course > 🧑 NetSec 2020 Student Issues > Issues > New

## New Issue

**Title** [exercise-hand-in] Exercise 1

**Description**

Write Preview

# Exercise sheet 1: Crypto and Networks refresher

## Crypto refresher

### Question 1

Concisely answer the following questions:

##### Question 1.1 (2 points)

Edward wants to prove to Laura he really is the sender of a message. What security property is he trying to achieve? Which cryptographic primitive could he use?

\*\*Solution:\*\* He could do a rain dance

Markdown and quick actions are supported

Attach a file

This issue is confidential and should only be visible to team members with at least Reporter access.

Submit issue Cancel

## Email

**Please use GitLab issues whenever possible  
and do not send us email.**

Using issues allows for discussion, better tracking of questions, and more transparency!

# Hacking Lab

- Students can autonomously solve challenges on hacking lab.
- Solving the challenges is NOT mandatory and does NOT influence the final grade. Solving the challenges will provide some practical experience and may help with the exam.
- Hacking Lab will be explained more in detail in an exercise session.

# Projects

- There will be two projects
- The projects are mandatory and individual
- 20 % of the final grade will be determined by the projects
- Each project has an equal weight
  
- ACME Project:
  - Implement an Automatic Certificate Management Environment (ACME) client
  
- Defend-the-Flag Project:
  - Diagnose and patch a vulnerable server
  
- More information will follow in the exercise session.

# Exam in January/February

- **Time:** Written exam, 120 minutes
- **Language:** Q: English, A: German or English (your choice)
- **Exam materials:** No extra materials are permitted
- **Exam coverage:**
  - Lectures, guest talks, exercises, projects
- **What and how we assess:**
  - We cover most (if not all) course topics
  - Understanding of security concepts, techniques and attacks as well as the ability to suggest appropriate defense measures
- **The exam will probably take place on computers**

## Grading

- **Exam:** 80 % of grade
- **Projects:** 20 % of grade
  - The two projects are weighted equally.
  - Not handing in a project results in a 1 *for that project*.
  - → Not handing in the projects results in a maximum score of 5.00 for the course.

# Action Items for Network Security Students

- **Lecture registration (“Einschreibung”)**
  - Subscribe to “Network Security HS 2020” on <https://www.mystudies.ethz.ch/>

## Legal use of NetSec material

- Some knowledge, technologies, code usable for attacks, it is illegal to use them for criminal activities
- It is also illegal to make available such technologies and code without proper measures
- Only myStudies-registered students have access to the course materials