Network Security

Chapter 1

Prof. Dr.-Ing. Georg Carle
Dr. Heiko Niedermayer
Cornelius Diekmann, M.Sc.

Lehrstuhl für Netzarchitekturen und Netzdienste
Institut für Informatik
Technische Universität München

Version: June 13, 2015

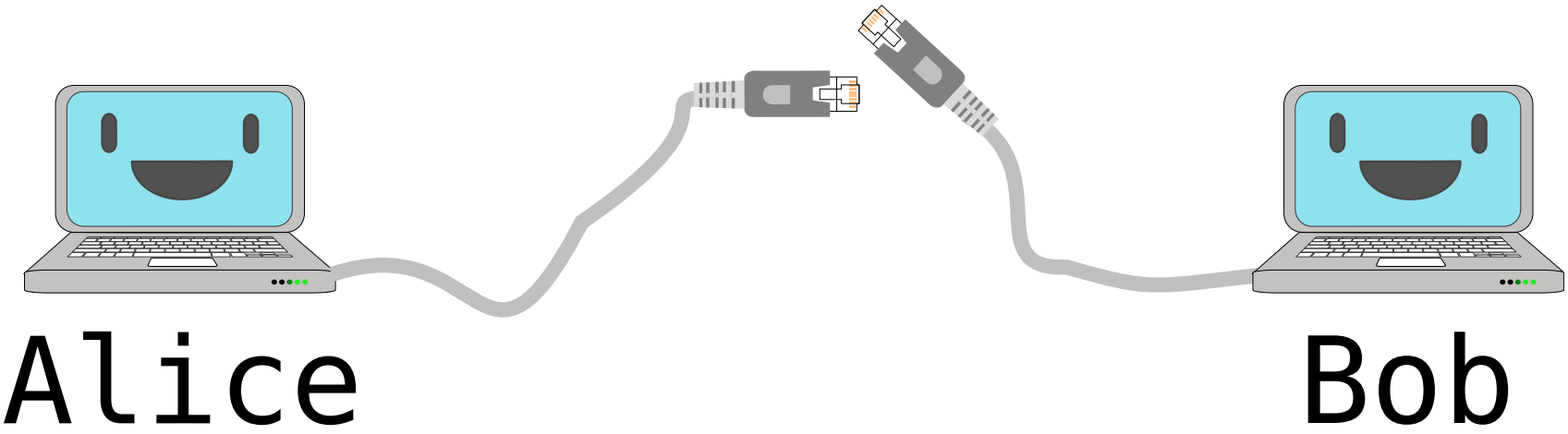
Introduction

Network InSecurity

- By example: An Ethernet cable
- How secure is it?

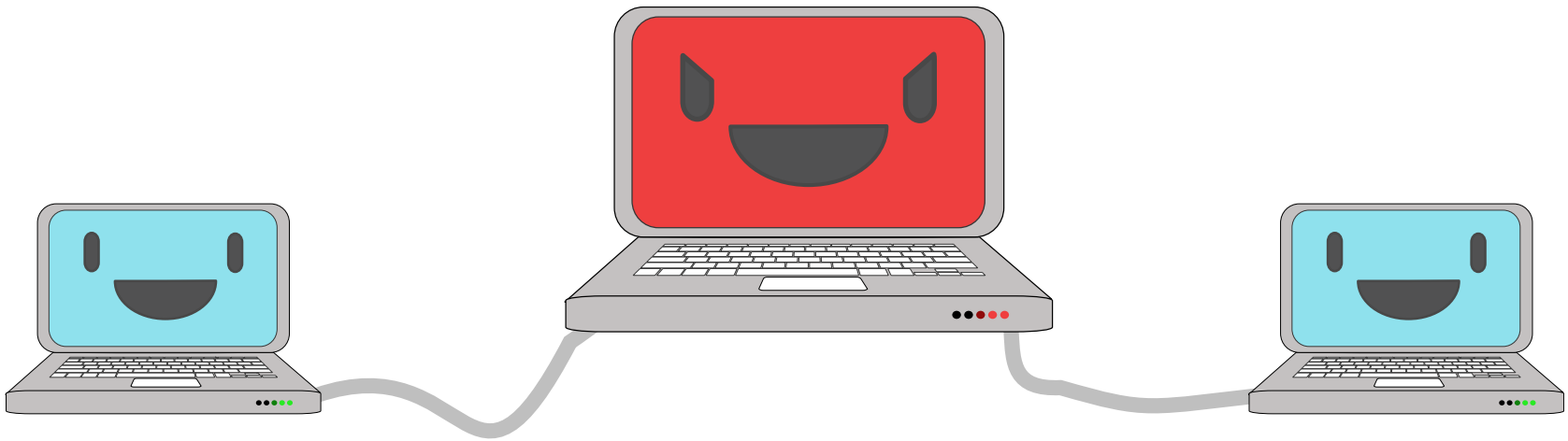
Network InSecurity

- Step 1: Obtain a knife
- Step 2: Add RJ45 adapters

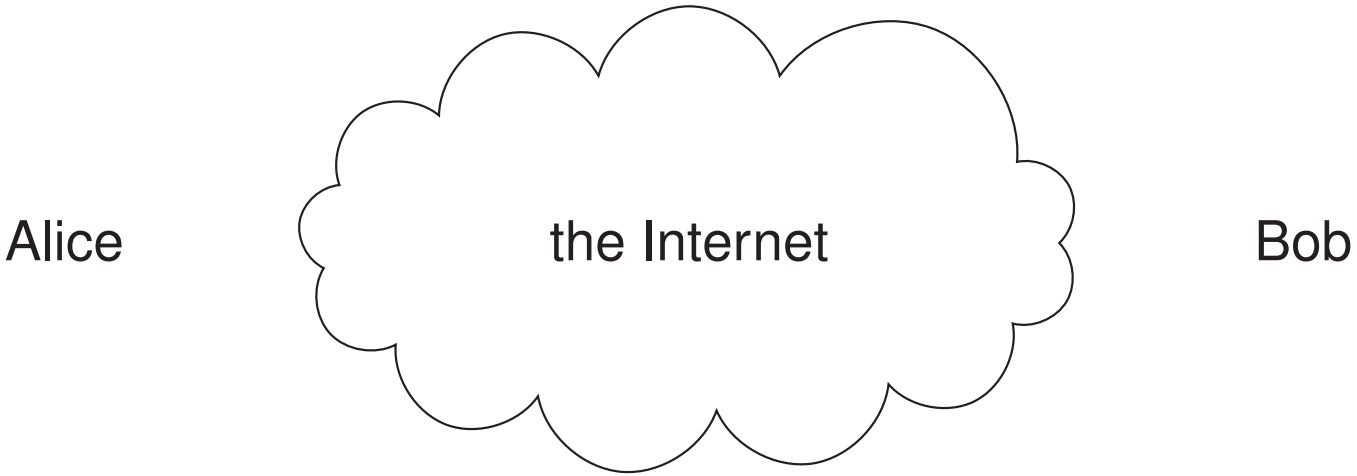


Network InSecurity

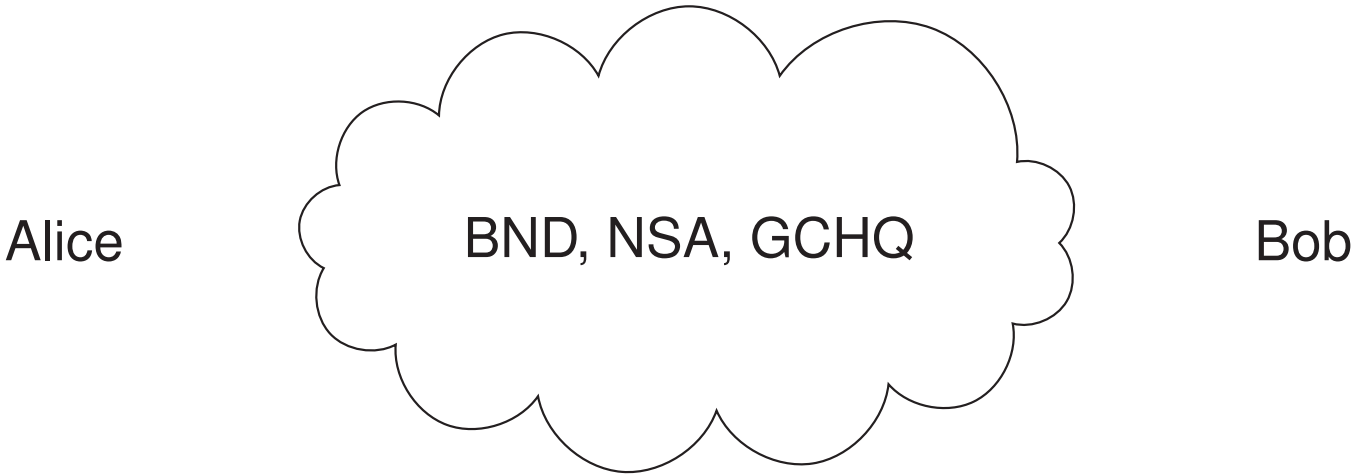
- Step 3: Configure transparent ethernet bridging
- You are now an in full control of the traffic
  - read
  - modify
- Technical term: *Man in the Middle* (MitM)



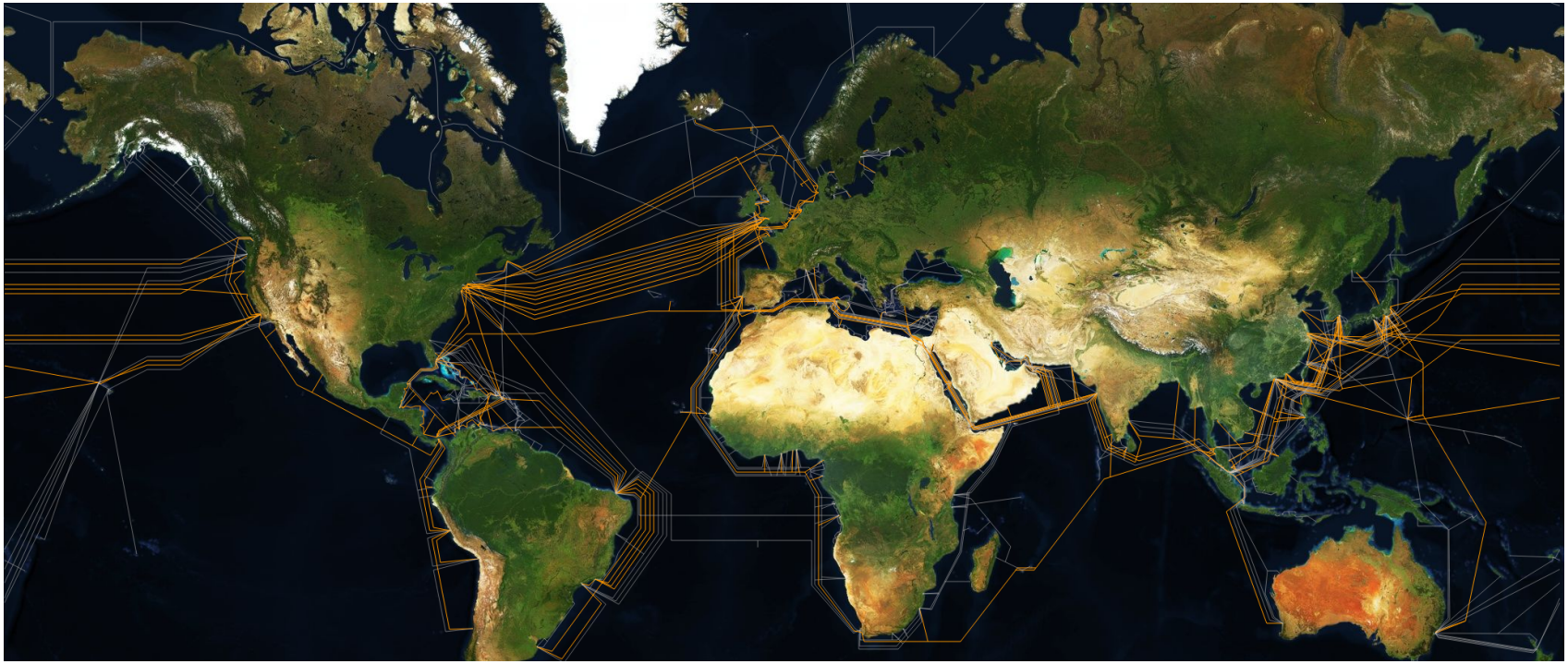
Network InSecurity



Network InSecurity



Network “Security” offered by our Secret Services



http://lifewinning.com/submarine-cable-taps/

- Passive attacks: wiretapping, . . .
- Active attacks: Quantum Insert, . . .
- Combined: economic espionage, . . .

Attackers

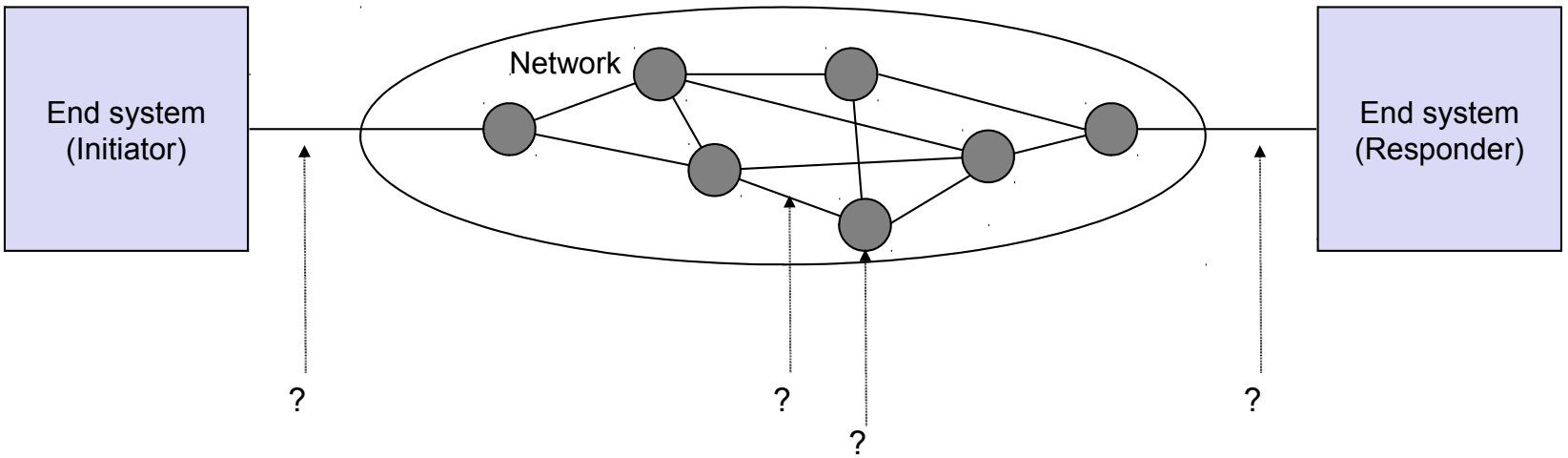
Attacker Models

- Attacking communications on the message level
- Passive attacks:
  - Eavesdropping of messages
- Active attacks
  - all passive attacks
  - Delay
  - Replay
  - Deletion
  - Modification
  - Insertion

General Attacker Model

- The attacker *is* the network
- And can perform any active attack
- But cannot break cryptographic primitives
- This is called the Dolev-Yao attacker model
- If not stated otherwise, we will always assume this attacker model.

Attackers Limited by their Position in the Network



Attackers Limited by their Position in the Network

- Assume the Attacker is close to you
- Example: You sit in a cyber cafe and accidentally connected to the attacker's hotspot
  - The attacker can perform any active attacks on you
  - But you can bypass this attacker: Establish a *secure* tunnel to a server in the Internet
  - Route all your packets over the secure tunnel
  - The attacker can now perform only DOS (Denial Of Service) attacks against you

Attackers Limited by their Position in the Network

- Assume the Attacker is close to your servers
- Example: She rented a VM on the same host machine where your virtual server is running
  - The attacker could try to perform timing attacks against you
  - By measuring how long certain operations take at your server, the attacker might be able to break a security service
  - (only if the service is vulnerable to side channel attacks)
  - Such measurement is usually not possible over the Internet

Attackers Limited by their Position in the Network

- Assume the Attacker is somewhere in the Internet
- Internet: Best effort packet switching
- End-user has no control how packets are routed
- Are all AS/ISP trustworthy?
- Does you ISP alter your packets?
  - “value added service” i.e. your ISP places advertisement on the websites you are visiting
- BND/NSA/GCHQ black boxes are basically everywhere

Security Goals

Security Goals Technically Defined

- Data Integrity
  - No improper or unauthorized change of data
- Confidentiality
  - Concealment of information
- Availability
  - Services should be available and function correctly
- Authenticity
  - Entity is who she claims to be
- Accountability german: „*Zurechenbarkeit*“
  - Identify the entity responsible for any communication event
- Controlled Access
  - Only authorized entities can access certain services or information

Quiz

- What is needed to support non-repudiation? („*Nicht-Abstreitbarkeit*“)

Quiz

- What is needed to support non-repudiation? („*Nicht-Abstreitbarkeit*“)
  - Accountability

Quiz

- What is necessary to support accountability?

Quiz

- What is necessary to support accountability?
  - Authenticity

Quiz

- What do you want to support deterrence („*Abschreckung*“)

Quiz

- What do you want to support deterrence („*Abschreckung*“)
  - Accountability

Quiz

- What is data origin integrity?

Quiz

- What is data origin integrity?
  - Authenticity

Quiz

- What it the difference?
- Authentication
- Authorization

Quiz

- What it the difference?
- Authentication
  - Proves who you are
  - Associated security goal: Authenticity
- Authorization
  - Defines what you are allowed to do
  - Associated security goal: Controlled Access

Quiz

- What it the difference?
- Authentication
  - Proves who you are
  - Associated security goal: Authenticity
  - E.g. your passport
- Authorization
  - Defines what you are allowed to do
  - Associated security goal: Controlled Access
  - E.g. “*are you on the VIP list?*”

Mixing Authentication and Authorization

My best attempt was registering to Black Hat with first name: "Staff" and last name: "Access All Areas"

https://twitter.com/mikko/status/587973545797492738

Threats

Threats

- Abstract Definition
  - A threat in a communication network is any possible event or sequence of actions that might lead to a violation of one or more security goals
  - The actual realization of a threat is called an attack

Threats Technically Defined

- Masquerade
  - An entity claims to be another entity (also called “impersonation”)
- Eavesdropping
  - An entity reads information it is not intended to read
- Loss or Modification of (transmitted) Information
  - Data is being altered or destroyed
- Denial of Communication Acts (Repudiation)
  - An entity falsely denies its participation in a communication act
- Forgery of Information
  - An entity creates new information in the name of another entity
- Sabotage/Denial of Service
  - Any action that aims to reduce the availability and / or correct functioning of services or systems
- Authorization Violation:
  - An entity uses a service or resources it is not intended to use

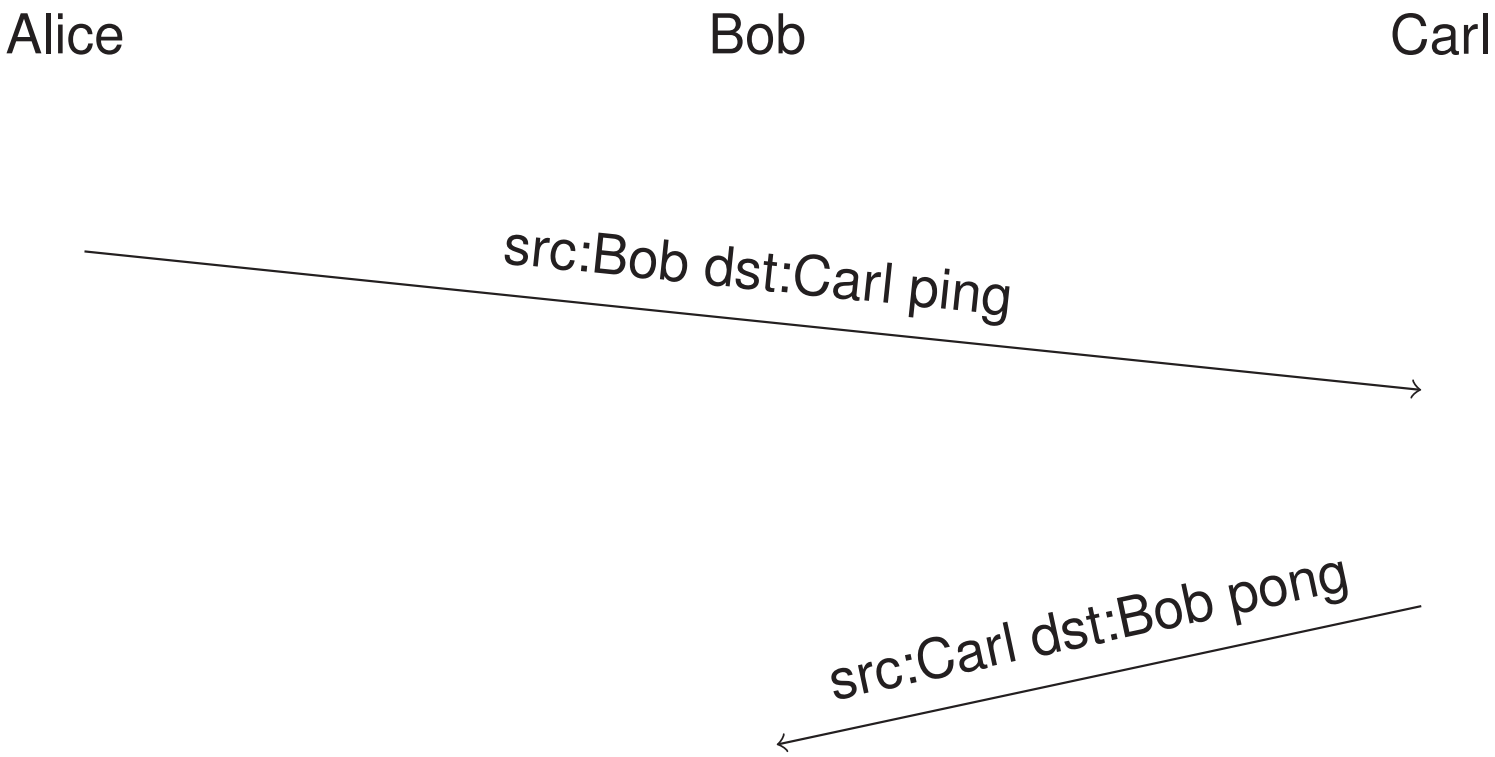
Example 1

- Eavesdropping + Authorization Violation
- Example
  - ```
    Alice@Box$ ./rootremoteshell $ROUTER
    root@router# tcpdump | grep password
    ```
- If Alice does not start modifying the traffic, she is a passive attacker
- Note: If not stated otherwise, we assume that attackers don't have remote code execution on our boxes
    ```

Example 2

- Masquerade + Forgery of Information
- Example
  - Alice pretends to be Bob
  - `Alice@Box$ hping3 --count 1 --spoof $BOB --icmp --icmptype 8 $CARL`
  - Bob gets an ICMP Echo Reply which he never requested
- Alice is an active attacker

Example 2: IP Spoofing cont.



Example 2: IP Spoofing cont.

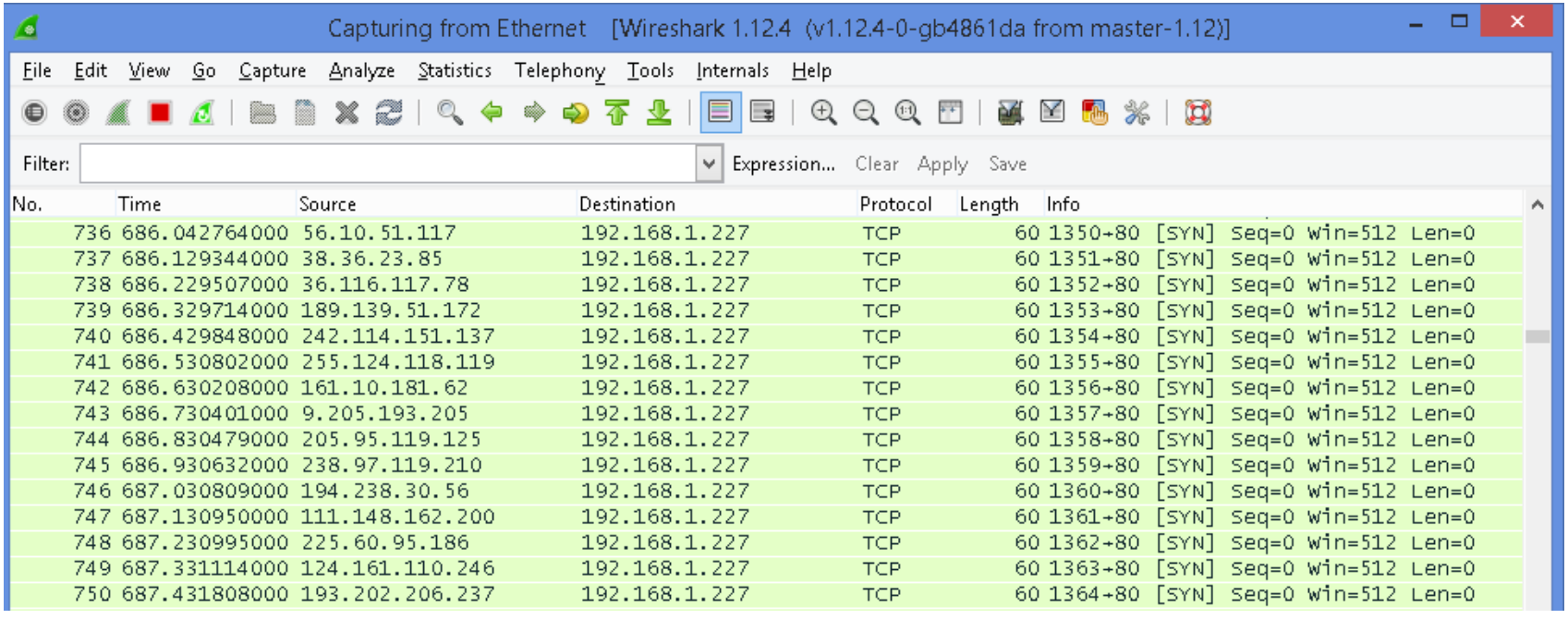
- Alice: 192.168.1.170
- Bob 192.168.1.227
- Carl: 192.168.1.1
- Alice sends the spoofed packet
  - Internet Protocol Version 4, Src: 192.168.1.227, Dst: 192.168.1.1; ICMP Echo Request
- Carl replies to the source address specified
- Bob receives a lonely echo reply
  - Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.227; ICMP Echo Reply

```
192.168.1.1          192.168.1.227          ICMP          60 Echo (ping) reply    id=0xce1f, seq=0/0, ttl=61
```

Example 3

- Denial of Service
- Example
  - Bob runs a webserver (http, tcp port 80) with very few memory
  - Alice floods Bob with TCP SYN packets
  - `Alice@Box$ hping3 --fast --count 42 --syn --destport 80 $BOB`
  - Bob allocates memory to store the 42 connections in the SYN-RECEIVED state
- Now Alice starts to deny that she is responsible for the attack
- Denial of Service + Forgery of Information + Denial of Communication Acts
- Example
  - `Alice@Box$ hping3 --fast --count 42 --rand-source --syn --destport 80 $BOB`
  - `--rand-source`: random spoofed source IP address

Example 3



- Why does the attack succeed?
- This is a good opportunity to refresh your knowledge about the TCP 3-way handshake

Literature

- Matt Bishop, *Introduction to Computer Security*, Addison-Wesley, 2004
- Claudia Eckert, *IT-Sicherheit: Konzepte – Verfahren – Protokolle*, Oldenbourg, 2014
- Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World (2nd Edition)*, Prentice Hall, 2002
- Matt Bishop, *Computer Security: Art and Science*, Addison-Wesley, 2002
- Günter Schäfer, *Security in Fixed and Wireless Networks: An Introduction to Securing Data Communications*, Wiley, 2004
- Günter Schäfer, *Netzsicherheit*, dpunkt, 2003