Forschungspraktikum Netz sicherheit
Forschungspraktikum

Forschungspraktikum Netz sicherheit

- Target audience: Students of Computer Science (Master)
- 3 ETCS
Before we start…

- Course will be given primarily in **German**
  - I.e., discussions etc. will be in German

- Material / Slides / Reports will be done in **English**
Before we start…

- **Mailing list**
  - Will be available shortly: fpns2021@ira.uni-karlsruhe.de
  - Will be used for announcements and coordination
  - Can also be used for any other discussions as well

- **Organizational inquiries**
  - Directly to the supervisors
Agenda for the Kick-Off-Meeting

- What is this practical course about?
- Time schedule
- Overview of graded documents/activities
- Next Steps
Agenda for the Kick-Off-Meeting

- What is this practical course about?
- Time schedule
- Overview of graded documents/activities
- Next Steps
Border Gateway Protocol (BGP)

- BGP is the de-facto standard for inter-domain routing in the Internet
  - Establishes connectivity between autonomous systems (AS)

- Standardized by the IETF (many different RFCs...)

- Main purpose of the protocol
  - Exchange reachability information
  - Which network (prefix) can be reached and how (path)
Border Gateway Protocol (BGP)

- How it works in principle (simplified!!!)
  - AS1 wants to communicate to AS2 that it can handle traffic regarding a specific prefix (say 1.2.3.0/24)
    - Does not necessarily mean that AS1 „owns“ this prefix
    - Only says that AS1 wants to receive traffic sent towards the prefix
  - AS1 must have a BGP Session established with AS2
  - AS1 then sends an UPDATE message for the given prefix towards AS2
  - AS2 receives the UPDATE message
    - Contains: prefix, path, next-hop
    - If AS2 accepts the message, the routing and forwarding table of the router(s) in AS2 may change so that traffic w.r.t. the prefix is sent towards AS1
Our Scope: BGP Security

- What can we observe from our point of view in BGP?
  - Misconfigurations that impact parts of the Internet
  - Misuse of BPG by malicious operators
    - Can we detect attacks?

- In this course, we …
  - want to understand important historical events in BGP
    - Outages, security incidents, …
  - want to study/observe such events in real monitoring data
  - want to make further use of the available data
    - This is the „research“ aspect
    - Could go into the direction of visualization, analysis, prediction, ...

- Application of machine learning techniques possible?
Overall Structure of the Course

- Part 1: Background and Preparations
  - 3 weeks

- Part 2: Working with the Data
  - 8 weeks

- Part 3: Wrap-up
  - 2 weeks + 3 weeks for report

➔ On-hands part is finished at the end of the semester
Part 1: Background and Preparations

Before we can go into more detail, we have to understand the basics.

We will work on the following questions in the first 2-3 weeks:

- How does BGP work?
- What are general observations we can make?
- What kind of data can we use in the remainder of the course?
  - How is this data structured?
  - What is relevant for us?
  - What conclusions can we draw from our observations?
Part 1: Background and Preparations

- Log example that we will understand after part 1

2016/12/31 06:28:34 BGP: 212.227.117.13 KEEPALIVE rcvd
2016/12/31 06:28:34 BGP: 212.227.117.13 rcvd UPDATE w/ attr: nexthop 212.227.117.13, origin i, path 8560 3257 3356 31133 28968 48098
2016/12/31 06:28:34 BGP: 212.227.117.13 rcvd 195.128.159.0/24
2016/12/31 06:28:34 BGP: 212.227.117.13 rcvd UPDATE w/ attr: nexthop 212.227.117.13, origin i, path 8560 2914 3356 31133 28968 48098
2016/12/31 06:28:34 BGP: 212.227.117.13 rcvd 195.128.159.0/24
2016/12/31 06:28:34 BGP: 212.227.117.13 rcvd UPDATE w/ attr: nexthop 212.227.117.13, origin i, path 8560 3257 174 31133 28968 48098
2016/12/31 06:28:34 BGP: 212.227.117.13 rcvd 192.166.96.0/22
Part 2: Working with the Data

- One main goal: use real world data
  - Part 1 focuses on general operation principles
  - Part 2 will now work with concrete data sets in more detail

2.1 Define a goal what do we want to find / achieve
  - Find specific anomalies in the data
  - Visualize certain aspects of the data
  - ...

2.2 Brief analysis of the goal
  - Is this possible to realize in the given timeframe?
  - What do we need? Tools? Methodology?

2.3 Implement / Experiment
  - We aim at small prototypes here! (Nothing too fancy)
Part 3: Wrap-up

- How to present the results of the course

- Should consists of two parts in general:
  - A short presentation about the results
    - Including a live demonstration
  - A brief report (3-5 pages)
Agenda for the Kick-Off-Meeting

- What is this practical course about?
- Time schedule
- Overview of graded documents/activities
- Next Steps
# Preliminary Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Meeting</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>Apr. 14(^\text{th}), 2021</td>
<td>Kick-Off-Meeting</td>
</tr>
<tr>
<td>2nd</td>
<td></td>
<td>Discussion BGP</td>
</tr>
<tr>
<td>3rd</td>
<td></td>
<td>Part 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Discussion BGP + Attacks/Anomalies</td>
</tr>
<tr>
<td>4th</td>
<td></td>
<td>Discussion BGP + Data</td>
</tr>
<tr>
<td>5th</td>
<td></td>
<td>Part 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Define Goal (1w)</td>
</tr>
<tr>
<td>6(^{th})</td>
<td></td>
<td>Part 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Goal Analysis (1w)</td>
</tr>
<tr>
<td>7th-11th</td>
<td></td>
<td>Goal Implementation (5w)</td>
</tr>
<tr>
<td>12th</td>
<td></td>
<td>Part 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prepare Presentation</td>
</tr>
<tr>
<td>13th</td>
<td></td>
<td>Part 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Presentation in last meeting</td>
</tr>
<tr>
<td>14th</td>
<td></td>
<td><strong>End of semester</strong></td>
</tr>
<tr>
<td>15th</td>
<td></td>
<td>Deadline final report</td>
</tr>
</tbody>
</table>
Agenda for the Kick-Off-Meeting

- What is this practical course about?
- Time schedule
- Overview of graded documents/activities
- Next Steps
Overview of graded documents/activities

- So what has to be done during the course?
  - Participation in the mandatory weekly meetings
  - Interim reports/presentations (unstructured)
    - During the weekly meetings
    - E.g., slides + discussions
  - Small (!) prototype that does something with the BGP data (code)
  - Final presentation
  - Brief report (3-5 pages)
Any Questions?

Contact

Hauke Heseding: hauke.heseding@kit.edu