2020-04-22

Forschungspraktikum Netzsicherheit

- Today: Information Event
- 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
- Modulhandbuch
  - Should be available shortly
  - Kennung: M-INFO-105413 Forschungspraktikum Netzsicherheit

Before we start…

The team:

- Robert Bauer (Organizer)
- Hauke Heseding (Organizer)
- Pascal Wagenblaß (Hiwi)

⇒ All organizational questions go towards Robert

Mailing list:

- We will set up a mailing list (fpns2020@ira.uni-karlsruhe.de)
- Will be used for announcement
- Can also be used for any other discussions as well

Agenda for Today

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

Agenda for Today

- **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
- Standardized by the IETF (many different RFCs...)
- Main purpose of the protocol
  - Exchange reachability information
  - Which network (prefix) can be reached and how (path)
- 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 wrt. the prefix is sent towards AS1

Our Scope: BGP in a Security Context

- It is not always clear who is „allowed“ to sent updates for a certain prefix

- This can cause significant problems
  - Configuration errors can cut off parts of the Internet
  - Malicious operators can use BGP to manipulate routes in the Internet

- In this course, we
  - want to understand what kind of attacks are possible with respect to BGP
  - want to discuss real attacks from history in detail
  - want to study/observe such attacks 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, prediction, ...

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 the general attack vectors?
  - What kind of data can we use in the remainder of the course?
    - How is this data structured?
    - What is relevant for us?

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 195.128.159.0/24

2016/12/31 06:28:35 BGP: 212.227.117.13 rcvd UPDATE w/ attr: nexthop 212.227.117.13, origin i, path 8560 1299 3356 31133 28968 48098

2016/12/31 06:28:35 BGP: 212.227.117.13 rcvd 195.128.159.0/24

2016/12/31 06:28:35 BGP: 212.227.117.13 rcvd UPDATE w/ attr: nexthop 212.227.117.13, origin i, atomic-aggregate, aggregated by 51088 46.244.0.134, path 8560 51088

2016/12/31 06:28:35 BGP: 212.227.117.13 rcvd 192.166.96.0/22

Part 2: Working with the Data

- One main goal is it to use real world data
- While we already made ourselves familiar with the way how BGP monitoring data looks like in general part 1, we will now work with concrete data sets in more detail

  - 2.1 Define a goal what do we want to find / achieve
    - Find specific attacks / anomalies in the data
    - Visualize certain aspects of the data
    - ...
  - 2.2 Brief analysis of the goal
    - Is this possible?
    - Is this realistic (only 3 credit points!!!)?
    - What do we need? Tools? Methodology?
  - 2.3 Implement / Experiment
    - We target at very small prototypes here!
    - Nothing too fancy

Part 3: Wrap-up

- How to present the results of the course
- This is not yet finalized, may change based on how the course develops
- Should consists of two parts in general:
  - A short presentation about the results
  - A brief report (3-5 pages)

Agenda for Today

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

Schedule (preliminary)

WN	Date	Meeting
17	2020-04-21	Today (30m)
18	Part 1	Discussion BGP
19		Discussion BGP + Attacks
20		Discussion BGP + Data
21+22	Part 2	Define Goal (2w)
23		Goal Analysis (1w)
24-28		Goal Implementation (5w)
29	Part 3	Prepare Presentation
30		Presentation in last meeting
30	2020-07-24	**End of semester**
33	Part 3	Deadline final report

Agenda for Today

- 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 (tbd) 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)

Agenda for Today

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

Next Steps

- I‘ll send around a mail with the **final registration**
  - To participate, answer to this mail with „Yes, I‘ll participate“
  - If you don‘t want to participate:
    - Please answer with „I will not participate“
    - No further steps are required then from your side

- Afterwards:
  - Participate in the Foodle that will be sent out later (for the weekly meeting)
  - Register online (student/campus portal)
  - Attend next weeks meeting

- That‘s it for now I guess…

Any Questions?

Contacts:

- Robert Bauer <robert.bauer@kit.edu>
- Hauke Heseding <hauke.heseding@kit.edu>