TRACE THE WUMPUS

PhD School | TMA Conference 2024

Johann Schlamp
An exciting simulated hunt in a hidden maze of caverns and twisting tunnels! Seek out the lair of the Wumpus, while avoiding perils along the way!
About me

Important milestones

1984–2003
Born and raised in a small village near Neuburg a.d.Donau with a strong allegiance to my homeland

2004–2009
Studied computer science with a minor in mathematics at the Technical University of Munich (TUM)

2009–2015
Doctorate at the Chair of Network Architectures and Services at TUM on architectural threats to Internet routing

Since 2014
Founder and CEO of Leitwert GmbH, since 2016 based in Ingolstadt
Lecturer at the Technische Hochschule Ingolstadt (THI)
About Leitwert

Many years of expertise on network analysis

- Founded in 2014 by a young team of network scientists
- Applied research and development for governments and industry
- Our goal: global inventory of Internet infrastructures and routing

World-wide measurement infrastructure

- We operate hardware at all major ISPs and Internet exchange points in Europe
- Our measurement infrastructure captures several billion routing changes – every day
- Raw data is carefully post-processed and enriched with manifold meta information
- Our data is suitable to study short-term network changes and long-term trends

Highest scientific standards

- Several internationally renowned publications on routing analysis
- Cooperative efforts with leading German universities
  with respect to research and teaching
Leitwert infrastructure

- New York
- Singapore
- Milan
- Cairo
- Singapore
- New York
- Telia
- Level3
- NTT
- Level3
- All rights reserved.
Leitwert measurements (I)

Conventional approach

Network maps based on publicly available measurement nodes
**Leitwert measurements (1)**

**Conventional approach**

Network maps based on publicly available measurement nodes
Leitwert measurements (1)

Conventional approach

Network maps based on publicly available measurement nodes
**Leitwert measurements (1)**

**Conventional approach**

Network maps based on publicly available measurement nodes
Leitwert measurements (II)

Real-world situation
Peering/transit-based Internet hierarchy
Leitwert measurements (III)

Our measurement approach

Active and passive network measurements at IXP/ISP- and router-level

Global top-down view at Leitwert
Post-processing and analytics

Continuous data enrichment
- Integration of virtually all publicly available network data
- Correlation with orthogonal routing data sets

Historic data archive
- Measurements and meta data since 2015
- Post-processed database exports since 2016
- Data archive comprising 100 TB network data

Analytical possibilities
- Machine learning – pattern recognition, anomalies, forecasts
- Physical inference – IP geolocation, router identification, submarine cables
- Forensics and attack detection – power outages, route hijacking, denial of service
- Policy evaluation – patented network analytics (EPO 3 430 775 / 2017-10-03)
Data access and evaluation

Available interfaces

- Raw data in MRT/JSON format
- Pre-processed database exports
- Web/HTTP-based REST API
- Python-based JSON-RPC API
- Interactive analysis frameworks

```
TABLE_DUMP_V2|131.159.0.0/16|19151 13030 680|IGP
db.daily_1610496000_ip.paths.find({hops: 131.159.15.50})
GET /api/v1/path/ip?target=131.159.15.50 & collector=level3
Query.path.ip(target=131.159.15.50, collector=level3)
tailored development based on individual needs
```
Research task #1
Vulnerabilities of the Internet infrastructure

Analysis
Review of outage reports, scientific results, marketing material etc.

Research task #2
Infrastructural, economical, and social changes

Evaluation
Measurement-driven approach to bolster analysis results

Auslandsverbindungen und CDN-Kompetenz (ZwIBACK)
Zweite Internet Backbone-Studie – Projekt 415 Los 1
PRIMEnet

Predictive analysis of routing and traffic flows for an intelligent network management

Aug 2021 – Jul 2024
Volume: 2.54 mio. Euro
KMU-innovativ
Information and communication technology (IKT)

Volume: 6.08 mio. Euro

Strengthening national cyber infrastructures with a cooperative Internet situation and information center

ALL#HANDS
Technical background

TRACEROUTE
Background – Active IP path measurements (I)

Traceroute: standard tool since the ‘80s (van Jacobson)

- Successive IP packets with **increasing time-to-live** (TTL) header value starting at 1
- Path reconstruction based on hop-wise TTL errors sent by intermediate routers
- Error messages defined in the **Internet Control Message Protocol (ICMP)**

Sample measurement

~$ traceroute www.net.in.tum.de
traceroute to www.net.in.tum.de (131.159.15.50), 30 hops max, 60 byte packets

```
1 vl500.dcata-017.as6724.net (85.214.1.25)    0.656 ms  1.088 ms  1.066 ms
2 be17.433.core-b1.as6724.net (85.214.0.168) 2.769 ms  2.738 ms  2.718 ms
3 ddn.bcix.de (193.178.185.42)    14.656 ms  14.644 ms  14.624 ms
4 zr-erl1-te0-7-0-1.x-win.dfn.de (188.1.145.145)    16.309 ms  16.295 ms  16.276 ms
5 xr-gar1-te3-1.x-win.dfn.de (188.1.144.249)    20.204 ms  20.675 ms  20.656 ms
6 kr-lrz-muenchen2.x-win.dfn.de (188.1.37.90)    20.128 ms  20.066 ms  20.357 ms
7 vl-3010.csr1-kw5.lrz.de (129.187.0.150)    23.323 ms  **
8 gatekeeper.informatik.tu-muenchen.de (131.159.252.1)    21.210 ms  21.200 ms  21.403 ms
9 nz-net-bb.informatik.tu-muenchen.de (131.159.252.150)    20.142 ms  20.146 ms  20.138 ms
10 www.net.in.tum.de (131.159.15.50)    20.070 ms  20.069 ms  20.044 ms
```
Background – Active IP path measurements (II)

A variety of challenges

- **Frequent artifacts** (e.g. missing replies, rate limiting, RFC1918 addresses, loops etc.)
- **Dynamic path changes** (e.g. load balancing, failover, route flapping etc.)
- **Path asymmetries** and invisible cross-links (mostly tree-like results)
- No notion of routers with IP interfaces (/31 practice, IPv4/IPv6, default interface etc.)
- **Problematic round trip times** (buffers, tunnels, one-way assumptions etc.)

A variety of solutions

- Paris traceroute
- Tracepath
- Smoketrace
- Scamper
- RIPE ATLAS
- IXP Jedi
- MTR
Background – Active IP path measurements (II)

A variety of challenges

- Frequent artifacts (e.g. missing replies, rate limiting, RFC1918 addresses, loops etc.)
- Dynamic path changes (e.g. load balancing, failover, route flapping etc.)
- Path asymmetries and invisible cross-links (mostly tree-like results)
- No notion of routers with IP interfaces (/31 practice, IPv4/IPv6, default interface etc.)
- Problematic round trip times (buffers, tunnels, one-way assumptions etc.)

A variety of solutions

- Paris traceroute
- Tracepath
- Smoketrace
- Scamper
- RIPE ATLAS
- IXP Jedi
- MTR
Background – Active IP path measurements (II)

A variety of challenges

- Frequent artifacts (e.g. missing replies, rate limiting, RFC1918 addresses, loops etc.)
- Dynamic path changes (e.g. load balancing, failover, route flapping etc.)
- Path asymmetries and invisible cross-links (mostly tree-like results)
- No notion of routers with IP interfaces (/31 practice, IPv4/IPv6, default interface etc.)
- Problematic round trip times (buffers, tunnels, one-way assumptions etc.)

A variety of solutions

- Paris traceroute
- Tracepath
- Smoketrace
- Scamper
- RIPE ATLAS
- IXP Jedi
- MTR
Now back on topic

HUNT THE WUMPUSS
Hunt the Wumpus (1973)

Interactive text adventure

- Move through a cave with interconnected rooms
- Shoot up to 5 crooked arrows through multiple rooms
- Sharpen your senses for natural drafts and telling smells
- Hunt down the Wumpus – or die facing numerous hazards

Dangerous environment

- Super bats in two rooms – random relocation
- Bottomless pits in two rooms – certain death
- Wumpus in one room – moves or kills when woken

Non-grid-like map

- 20 rooms with 3 tunnels per room
- Placed on vertices of a dodecahedron
Anyways – what is a Dodecahedron?

The regular dodecahedron

- One of five Platonic solids (together with tetrahedon, cube, octahedron, and icosahedron)
- Consists of 12 regular pentagonal faces, i.e. 20 vertices (rooms) and 30 edges (tunnels)
- Can be projected onto two dimensions using a Schlegel diagram or a Hamilton cycle
Trace the Wumpus (2024)

Original game

- 226 lines of **BASIC code** written by Gregory Yob in 1973
- Source code published in *Creative Computing* in 1975
- Several sequels and ports to various platforms

Revived game

- Screen of 63 x 20 characters using standard **Windows/Linux traceroute**
- Commands (game/move/shoot) modeled as forward DNS traceroute targets
- Output predefined via fixed strings registered in reverse DNS (complete game output!)
- Needs IPv6 due to a combinatory explosion of shoot commands (N out of 20)
- **Full game experience** on any machine without installing any software

Official release

- Planned **after the tutorial** – maybe today/tomorrow
- But cannot be played at TMA'24 (**no IPv6**) 😞
Requirements for participation

PROJECT MANAGEMENT
We are using Scrum!

The Scrum process in detail:
- Sprints of 2-4 weeks in a team of 3-9 developers
- Customer involvement for planning and review

Definition of »events«
- Sprint Planning: Selecting user stories and defining explicit tasks to be included in next sprint
- Sprint Review: Approving a product increment by the customer based on acceptance criteria
- Backlog Refinement: Improving and extending backlog with missing/newly identified features
We enforce a coding style

Conventions
- Code language is English
- Indentation with 4 spaces (no tabs)
- Maximum of 80 characters per line
- Double quotes for all strings
- Class and function documentation
- License header in all source files

Source code documentation
- Short description and author list
- Relevant background information
- List of arguments including types
- Description of return value
- List of raised exceptions
Requirements for participation

SEND NETWORK PACKETS
The new WUMPUS game (I)

[GOAL] Use your local traceroute tool and play

```bash
~$ traceroute6 play.wumpus.quest
traceroute to play.wumpus.quest (2a06:2904::10:10:11), 30 hops max, 80 byte packets
1  W-------------------------------------------------------------W (2a06:2907::ff:ff:cb)  6.285 ms
2  W--TRACE.THE.WUMPUS-------------------------------------------W (2a06:2907::ff:ff:c4)  12.055 ms
3  W-------------------------------------------------------------W (2a06:2907::ff:ff:cb)  17.244 ms
4  W--YOU.ARE.IN.ROOM-14------------------------------------------W (2a06:2907::ff:ff:95)  22.157 ms
5  W--TUNNELS.LEAD.TO-4-13-15-------------------------------------W (2a06:2907::ff:ff:b3)  28.317 ms
6  W-------------------------------------------------------------W (2a06:2907::ff:ff:cb)  32.640 ms
7  W--MOVE---move.ROOM.wumpus.quest-------------------------------W (2a06:2907::ff:ff:c9)  29.382 ms
8  W--SHOOT--shoot.ROOM1.ROOMX.wumpus.quest----------------------W (2a06:2907::ff:ff:ca)  29.474 ms
9  W-------------------------------------------------------------W (2a06:2904::10:10:11)  29.743 ms
```

```bash
~$ traceroute6 move.15.wumpus.quest
...
```

```bash
~$ traceroute6 shoot.16.20.13.wumpus.quest
...
```
We are building a server component

- Respond to packets with TTL exceeded from multiple IP addresses
- We need nothing else (no routing, no client, no DNS) – only packet crafting on layers 2-7

The new WUMPUS game (II)
The new WUMPUS game (II)

We are building a server component

- Respond to packets with TTL exceeded from multiple IP addresses
- We need nothing else (no routing, no client, no DNS) – only packet crafting on layers 2-7

```
~$ traceroute wumpus.quest
```

![Diagram showing network components andtraceroute command](#)
Let the games begin
WE'RE STARTING
Prepare for a multitude of mini-challenges

Conceptual problems

- Support any traceroute implementation (Linux/Windows, UDP/TCP, Paris traceroute etc.)
- Support arbitrary traceroute parameters (especially -q/ --queries and -m/ --max-hops)
- Map incoming packets to traceroute output lines and force measurement to stop

Technical hurdles

- Making first contact with Python3 (hopefully not!)
- Getting the routing right – should be solved by `docker compose`
- How to efficiently filter and assemble packets on layers 2-7?

Game play challenges

- Navigate the dodecahedron (try to find a map)
- Shoot around the corner – but not yourself
- Find a suitable strategy without debug cheats
Getting your hands dirty

Project files
https://www.leitwert.net/code/wumpus.zip

First steps
- Download and unzip project files
- Change to project directory
- Run `docker compose build`
- Run `docker compose up`

Your tasks
- Inspect and edit `src/trace.py` (Docker entry point)
- Capture and print packets inside the container
- Implement ICMP `ping` for incoming echo requests
- Implement ICMP `traceroute` for incoming TCP/UDP requests
- Rewrite both routines to support `ICMPv6` ping/traceroute

[bonus task]
Use ICMP MPLS extensions to encode debug game state

```python
# Local imports
from wumpus.game import Game
from wumpus.const import FILTER_PREFIX_IPV6
from wumpus.const import FILTER_PREFIX_IPV4

# Constants
INTERFACE = "eth0"

# Globals
game = Game(debug=True)

# Sample game input
src, dst = "2001::1", "2a06:2904::10:10:10"
hops = game.handle_input(src, dst)
```
Model solution has less than 100 lines of code 😊

Your tasks for today

ping4 ⇨ traceroute4 ⇨ ping6 ⇨ traceroute6

Additional hints [provided every ~10 minutes]
Model solution has less than 100 lines of code 😊

Your tasks for today: https://www.leitwert.net/code/wumpus.zip

- ping4 ⇔ traceroute4 ⇔ ping6 ⇔ traceroute6

Additional hints [provided every ~10 minutes]

- Use Python scapy
  ```python
  from scapy.all import sniff
def callback(pkt):
    pkt.show()
  sniff(iface=INTERFACE, prn=callback, filter=f"net {FILTER_PREFIX_IPV6} or net {FILTER_PREFIX_IPV4}"")
  ```

- Get layer 2 right first
  ```python
  from scapy.all import Ether, UDP, TCP, Raw
  from scapy.all import ARP, IP, ICMP
  from scapy.all import IPv6, ICMPv6ND_NS, ICMPv6ND_NA, ICMPv6NDOptDstLLAddr
  from scapy.all import ICMPv6EchoRequest, ICMPv6EchoReply, ICMPv6TimeExceeded, ICMPv6DestUnreach
  ```

- ICMP packets need a payload that mirrors incoming packets
- Keep track of changes in ttl / hop limit header values per client
- Terminate measurements with ICMP destination unreachable
OOPS – BUMPED A WUMPUS
THANK YOU