BTI 7311 Seminar Topics 2018

Christian Grothoff

Berner Fachhochschule

March 3, 2018

Fuzzing[1]

- Fuzzing is a traditional technique to find vulnerabilities
- AFL is a modern fuzzing tool
- Literature proposed various improvements
- Explain directed fuzzing and survey available tools

`https://arxiv.org/abs/1709.07101`

[1] David Michael Scheppard

Byzantine Fault Tolerant Random Peer Sampling[2]

- BRAHMS proposes a protocol for BFT RPS
- Explain BRAHMS
- Review related work (before, after)

`https://www.sciencedirect.com/science/article/pii/S1389128609001182`

[2] Daniel Schmitz

Rust[3]

- Give an introduction into the Rust language
- Present the Rust type system
- Focus should be on ownership types and traits

`https://people.mpi-sws.org/~dreyer/papers/rustbelt/paper.pdf`

[3] Jan Scheidegger

NAT Traversal[4]

- Internet middleboxes performing NAT are often an obstacle for end-to-end communication
- STUN/TURN/ICE are traditional NAT traversal methods
- Other methods include ALG (FTP-ALG, SIP-ALG) and hole punching
- Provide an overview of the state of the art in NAT traversal

`http://ieeexplore.ieee.org/abstract/document/6181044/`

[4] Florian Auderset

Spectre/Meltdown[5]

- Explain the vulnerabilities
- Explain the precise attack conditions
- Explain migigation techniques proposed and deployed

`https://arxiv.org/abs/1801.01203`

[5] Michel Utz

TCP congestion control[6]

- Survey TCP congestion control algorithms (beyond TCP Reno)
- Explain Bufferbloat and mitigations
- In particular, look into net2o

`https://dl.acm.org/citation.cfm?id=2063196`

[6] Ueli Bachmann

HTTP 2.0[7]

- Study motivations for and main changes in HTTP 2.0
- Survey performance studies comparing HTTP/1.1 and HTTP 2.0

`http://ieeexplore.ieee.org/document/7980103/`

[7] Denis Shevchenko