BTI 7311 Seminar Topics 2020

Christian Grothoff

Berner Fachhochschule

February 3, 2020

Penrose: Substance and Style

- Substance and Style are domain-specific languages for mathematical diagrams
- Paper was presented as SPLASHCON 2017
- Teach us how to use the DSLs to make great scientific diagrams!

`https://2017.splashcon.org/`

Searchable encryption

- We like to store data on servers.
- We don't trust servers, so we encrypt data on servers.
- But we need to search our files based on their contents.
- How can we search encrypted files without exposing the query or contents to the server?
- How can we make this fast? Present background and the latest results.

`https://petsymposium.org/2018/files/papers/issue1/paper11-2018-1-source.pdf`

Tracking using TLS client authentication

- TLS solves all of our security problems.
- Except for those it introduces.
- Apple enabled tracking of Apple users because of TLS.
- Explain the original attack, the fix, and the improved attack.

`https://petsymposium.org/2018/files/papers/issue4/popets-2018-0031.pdf`

Performance measurement

- Linux helps with performance measurement
- Perform *meaningful* benchmarks (ideas to be discussed with the instructor)
- Explain the Linux perf tool and results obtained

`http://www.brendangregg.com/perf.html`