BTI 7311 Seminar Topics 2019

Christian Grothoff

Berner Fachhochschule

November 28, 2018

HTTP/3

- HTTP/3 is being standardized by IETF based on Google's QUIC.
- HTTP/3 runs over UDP instead of TCP
- Explain changes to the congestion control protocol vs. TCP
- Find reference implementations and performance studies

`https://daniel.haxx.se/blog/2018/11/11/http-3/`

Penrose: Substance and Style

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

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

AMPL

- AMPL is a domain-specific language for mathematical programming, specifically operations research.
- There is the AMPL book (freely available online). Read it!
- Explain the problem domain with examples
- Explain the language

`https://ampl.com/`

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

- Performance measurement is hard
- Modern hardware makes it really hard
- Explain the sources of measurement errors
- Explain mitigations for proper measurements

`https://www.usenix.org/system/files/osdi18-maricq.pdf`

Performance measurement

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

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

TypeScript

- JavaScript is being replaced by TypeScript
- Give an introduction to the language
- Highlight key advantages
- Explain how TypeScript code integrates with legacy JavaScript

`http://www.typescriptlang.org/`

The GNU Linear Programming toolKit (GLPK)

- GLPK is a standard tool for solving linear optimization problems
- Explain what linear optimization is
- Show how to use libglpk to solve LPs and ILPs
- Some C knowledge required!

`https://www.gnu.org/s/glpk/`

RFC 8445: Internet Connectivity Establishment

- RFC 8445 describes ICE, a method for NAT traversal
- Explain the various components of ICE
- What changed since RFC 5245?
- Survey existing implementations of ICE

`https://tools.ietf.org/html/rfc8445`

ECCploit

- RowHammer was yesterday's attack on memory
- These days even ECC memory is no longer safe!
- Explain the ECCploit!

`https://cs.vu.nl/~lcr220/ecc/ecc-rh-paper-eccploit-press-preprint.pdf`