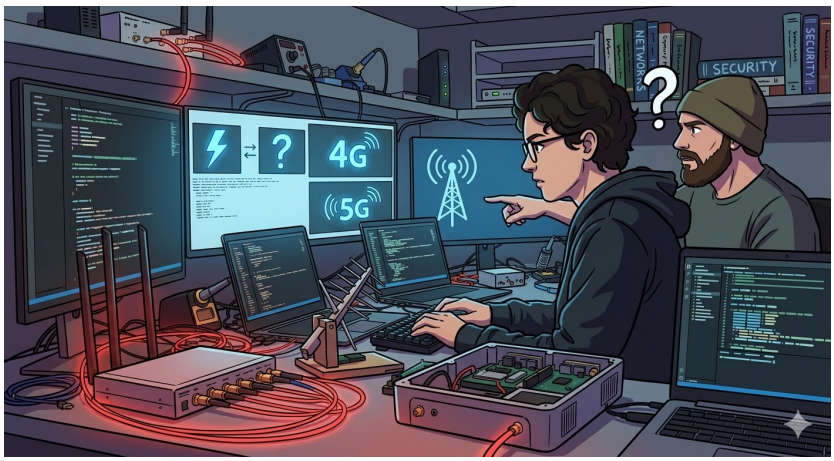
Log-driven fuzzing of 4G/5G protocols



The security of 4G and 5G cellular protocols is increasingly critical, yet the evaluation of proprietary modem implementations remains hindered by their closed-source nature. Traditional black-box fuzzing is an easy method for testing these devices; however, it is inherently limited by a lack of useful feedback for guiding the fuzzing process. To address this "blindness," this research proposes leveraging diagnostic modem logs as a feedback mechanism, similar to the previous research Logos [2]. Since most Qualcomm 4G/5G modems expose extensive debug logs that can be gathered using tools like QCDebugMonitor [1], these data streams can be utilized to optimize and direct fuzzing strategies.

The goal of this thesis is to improve an existing 4G/5G fuzzing framework written in C++ by integrating these log-driven fuzzing strategies. This will require the student to become familiar with the fundamentals of fuzzing, 4G/5G protocol stacks, and the internal architecture of modem firmware. During the thesis, the student is expected to (1) develop an algorithm that provides a feedback for the fuzzer based on the observed logs, (2) implement and integrate it into an existing fuzzing framework and (3) validate the framework's effectiveness by testing it against a variety of commercial 4G/5G modems to evaluate its bug-discovery performance.

[1] Dmytro Oleksiuk. Debug messages monitor for Qualcomm cellular modems. `https://github.com/Cr4sh/qc_debug_monitor`.

[2] F. Wu, Z. Luo, Y. Zhao, Q. Du, J. Yu, R. Peng, H. Shi, and Y. Jiang. Logos: Log guided fuzzing for protocol implementations. In *Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis*, ISSTA 2024, page 1720–1732, New York, NY, USA, 2024. Association for Computing Machinery.

Practicalities

Promotor:	Bart Preneel
Daily supervisor:	Ilja Siroš ilja.siros@esat.kuleuven.be office B01.17
Nature of the work:	20% literature, 80% software
Number of students:	1

 © 2026 – 2027 COSIC