**CONCLUSION**

We introduced four security rules that capture desirable properties of REST APIs and services. We then showed how a stateful REST API fuzzer can be extended with active property checkers that automatically test and detect violations of these rules. So far, we have fuzzed nearly a dozen production Azure and Office-365 cloud services using the fuzzer and checkers described in this paper. In almost all cases, our fuzzing was able to find about a handful of new bugs in each of these services. About two thirds of those bugs are “500 Internal Server Errors”, and about one third are rule violations reported by our new security checkers. We reported all these bugs to the service owners, and all have been fixed. Indeed, violations of the four security rules introduced in this paper are clearly potential security vulnerabilities. The bugs we found have all been taken seriously by the respective service owners: our current bug “fixed/found” ratio is nearly 100%. Moreover, it is safer to fix these bugs rather than risk a live incident – provoked intentionally by an attacker or triggered by accident – with unknown consequences. Finally, it helps that these bugs are easily reproducible and that our fuzzing approach reports no false alarms. How general are these results? To find out, we need to fuzz more services through their REST APIs and check more properties to detect different kinds of bugs and security vulnerabilities. Given the recent explosion of REST APIs for cloud and web services, there is surprisingly little guidance about REST API usage from a security point of view. Our paper makes a step in that direction by contributing four rules whose violations are security-relevant and which are nontrivial to check and satisfy.