Luciano Bello (joint work with Alejandro Russo)

Abstract
Cloud computing is generally understood as the distribution of data and computations over the Internet. Over the past years, there has been a steep increase in web sites using this technology. Unfortunately, those web sites are not exempted from injection flaws and cross-site scripting, two of the most common security risks in web applications. Taint analysis is an automatic approach to detect vulnerabilities. Cloud com- puting platforms possess several features that, while facil- itating the development of web applications, make it dif- ficult to apply off-the-shelf taint analysis techniques. More specifically, several of the existing taint analysis techniques do not deal with persistent storage (e.g. object datastores), opaque objects (objects whose implementation cannot be ac- cessed and thus tracking tainted data becomes a challenge), or a rich set of security policies (e.g. forcing a specific or- der of sanitizers to be applied). We propose a taint analy- sis for could computing web applications that consider these aspects. Rather than modifying interpreters or compilers, we provide taint analysis via a Python library for the cloud com- puting platform Google App Engine (GAE). To evaluate the use of our library, we harden an existing GAE web applica- tion against cross-site scripting attacks.