

SECURITY AND PRIVACY BY CONSTRUCTION WITH POLICY-AGNOSTIC PROGRAMMING

JEAN YANG
ASSISTANT PROFESSOR,
COMPUTER SCIENCE DEPARTMENT
CARNEGIE MELLON UNIVERSITY

Recent high-profile data breaches in systems spanning healthcare, insurance, and even the government have demonstrated the vulnerability of consumer data. Though worrisome, the prevalence of information leaks should be no surprise. Not only are users sharing more information, but there is a growing amount of code that handles sensitive data. Unless we make it easier to create secure programs, information leaks will only get worse.

As a solution to the problem of information leaks, we propose a new programming paradigm called policy-agnostic programming. In policy-agnostic programs, the programmer attaches security and privacy policies directly to sensitive data. In contrast, in existing languages, the programmer must implement policies as repeated checks and filters across the program—an error-prone and inefficient process. In policy-agnostic programs, the programmer needs to specify each policy only once and can then rely on the language implementation to automatically customize program behavior according to the policies. These policies can represent rules about how sensitive values may flow through a program—for instance, “Only friends may see Alices real GPS location.” The language implementation automatically ensures that program outputs adhere to the rules.

To demonstrate the practicality of policy-agnostic programming, we created Jacqueline, a web framework that enforces security and privacy policies in database-backed web applications. We proved that our technique ensures policy compliance across the application and database, tracking sensitive values and policies through all database queries, while requiring no modifications to a commodity relational database. We implemented Jacqueline using an unmodified Python interpreter and SQL database. Through several case studies and a real application deployment we show that Jacqueline reduces the amount of policy code required while incurring limited overheads.

This work validates the design and implementation of a policy-agnostic programming model. We hope to encourage others to think about tools that provide security and privacy by construction.

The work on the Jacqueline web framework is currently under submission [2]. We proposed the idea of policy-agnostic programming and presented the Jeeves programming language in earlier work [3, 1].

REFERENCES

- [1] Thomas H. Austin, Jean Yang, Cormac Flanagan, and Armando Solar-Lezama. Faceted execution of policy-agnostic programs. pages 15–26, 2013.
- [2] Jean Yang, Travis Hance, Thomas H. Austin, Armando Solar-Lezama, Cormac Flanagan, and Stephen Chong. End-to-end policy-agnostic security for database-backed applications. *arXiv.org*, cs.PL, 2015.
- [3] Jean Yang, Kuart Yessenov, and Armando Solar-Lezama. A language for automatically enforcing privacy policies. pages 85–96, 2012.