Provably Enforcing Practical Multi-Layer Policies in Today's Extensible Software Platforms

Limin Jia and Lujo Bauer Carnegie Mellon University

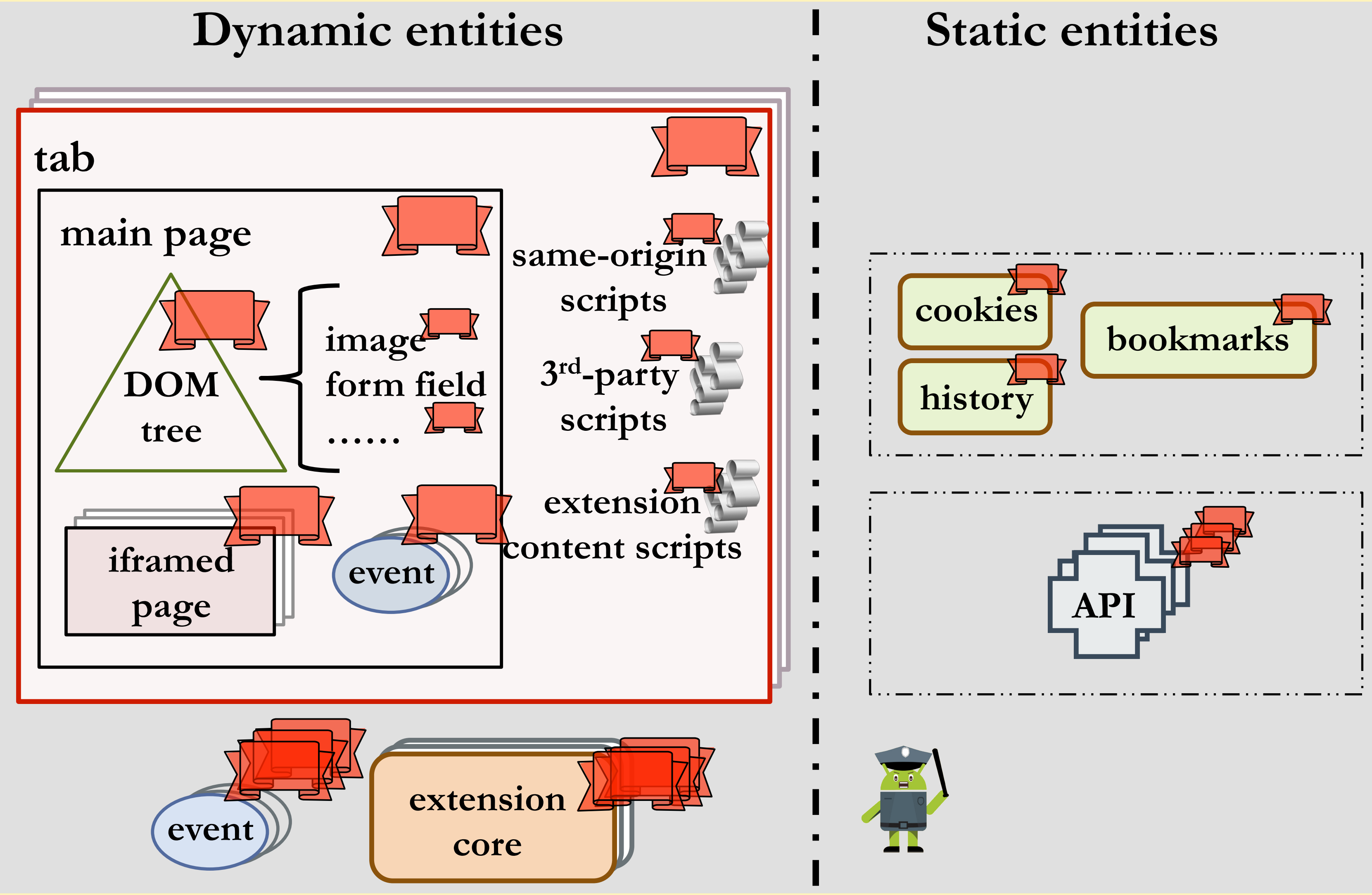
Securing extensible platforms

Modern software platforms such as Android OS and browsers are composed of a collection of components. These platforms can be further extended by additional third-party components. The goal of this project is to investigate how to enforce security policies on such platforms, taking into consideration the heterogeneity of the components.

- What types of policies can be efficiently enforced?
- How to compose/interface different enforcement mechanisms used for individual components?

Focus on browser platform (Chromium)

- Extensible via browser extensions
- Includes static and dynamic entities (illustrated on the right)



Approach

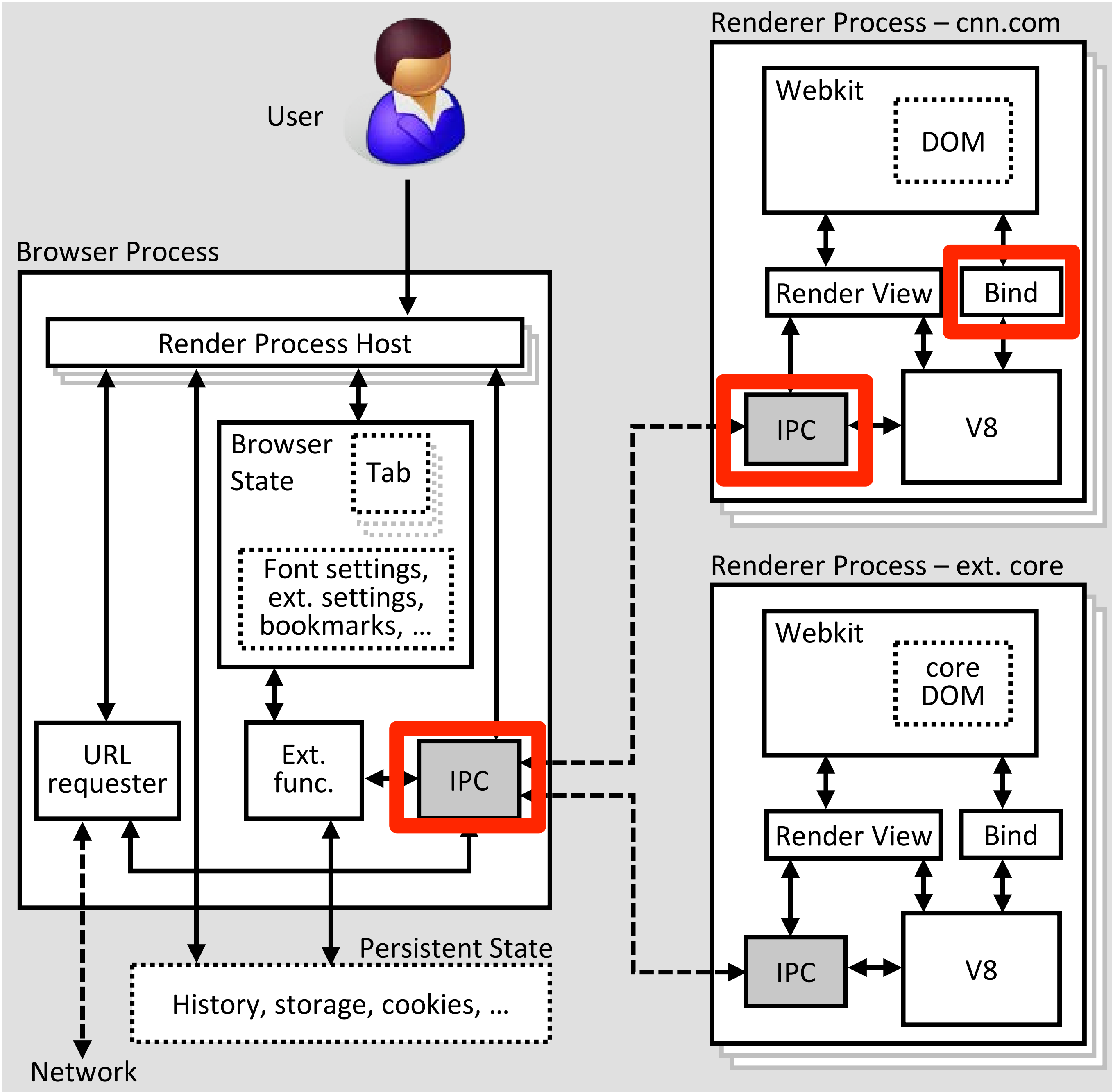
Information flow policies

- Protection secrecy of users' data and integrity of data that flows into key APIs
- Well studied in their compositional properties

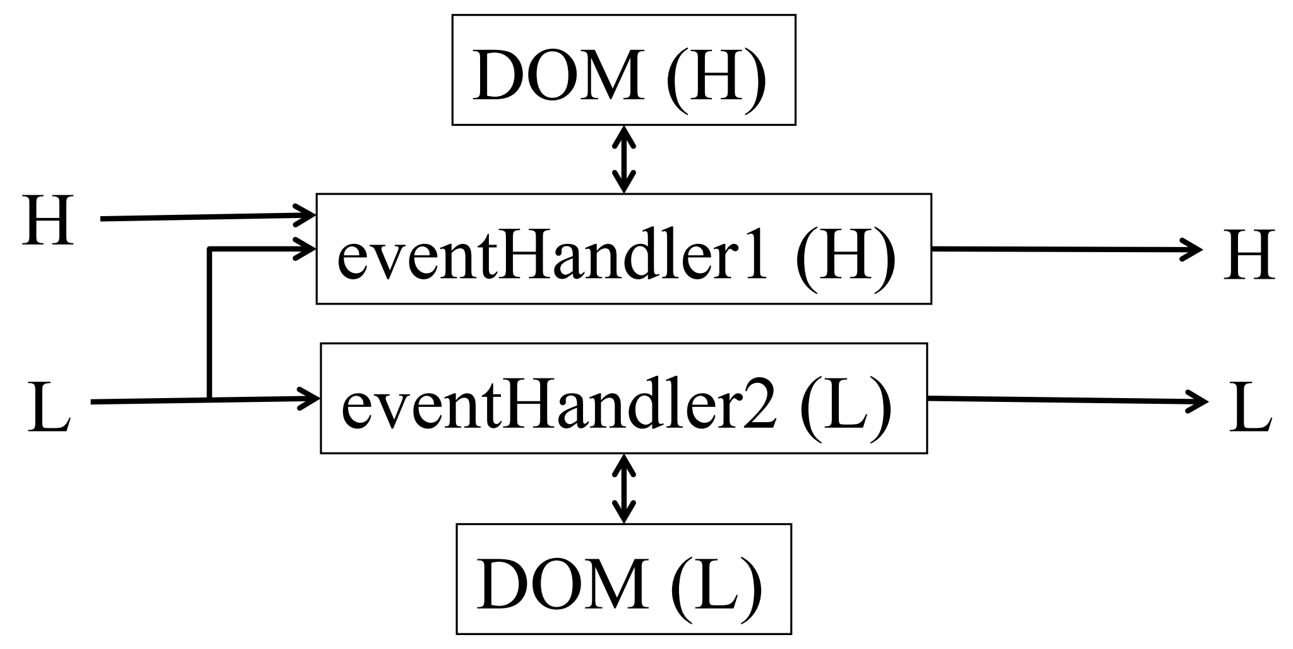
Interfacing enforcement mechanisms

- Runtime enforcement is practical for retrofitting existing systems
- Static enforcement avoids runtime overhead
- Utilize natural boundaries between components for interfacing

Coarse-grained tracking in Chromium



Secure multi-shared-state



Using the infrastructure to inform user

- Track from where scripts are loaded
- Track where each visual component is from
- Inform the user of the provenance via browser GUI modifications

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN

Carnegie Mellon University