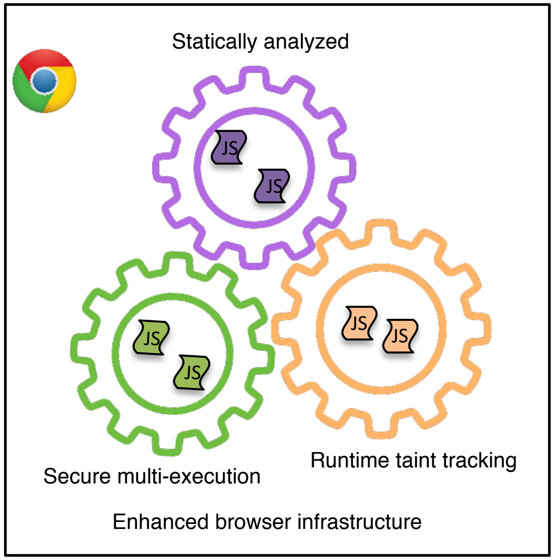
Towards a Usable, Practical, and Provably Secure Browser Infrastructure

Carnegie Mellon University
Security and Privacy Institute
CyLab

Challenge:

- Web applications are susceptible to XSS attacks, but few existing tools effectively help programmers or users to detect them
- Proposed security mechanisms for preventing web applications from leaking users' private information are one-size fit all and can't be easily used in practice



Solution:

- Improve browser infrastructure (Chromium) with taint tracking to help identify bugs and enforce security properties in web applications
- Develop compositional framework to combine existing information flow control (IFC) mechanisms to enforce IFC policies on web applications

Scientific Impact:

- The compositional framework could provide insight into how best to combine different IFC mechanisms to achieve desired efficiency and strength of security guarantees
- Results from this project can show where IFC succeeds and fails in ensuring the security and privacy of web applications

Broader Impact:

- Web-based attacks are becoming more and more common; results from this project have the potential to help not only web developers but all also web users
- Research results have been integrated into the curriculum of CMU course 18636/14828 Browser Security
- Our taint-tracking Chromium has been used as the basis for several undergraduate research projects

CNS1704542, Carnegie Mellon University
Limin Jia (PI), Lujo Bauer, Matt Fredrikson, Jean Yang