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

Carnegie Mellon University

Challenge:

- How to **provably enforce security policies** in platforms such as mobile OSes and browsers
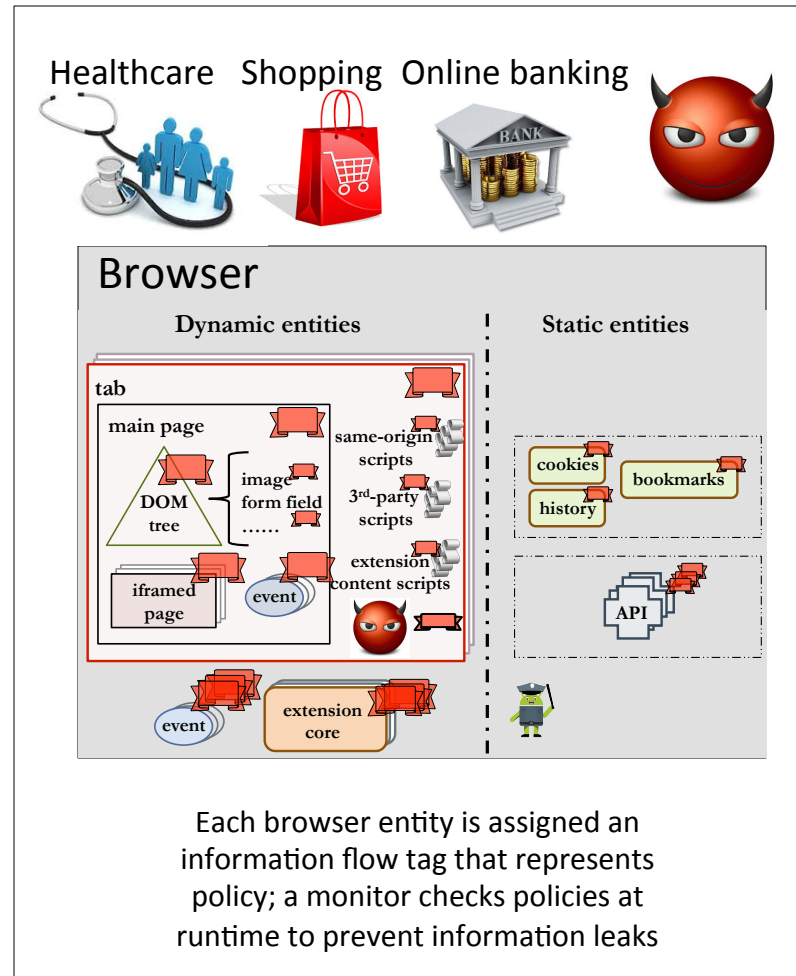- Platforms encompass heterogeneous components

Solution:

- Applied **coarse-grained distributed information flow** control to protect secrecy and integrity of user data and system resources
- Developed **prototype for Chromium** browser
- **Formally verified** security guarantees

CNS-1320470

Limin Jia (liminjia@cmu.edu)

Lujo Bauer (lbauer@cmu.edu)

Each browser entity is assigned an information flow tag that represents policy; a monitor checks policies at runtime to prevent information leaks

Scientific Impact:

- Demonstrated how to improve mobile OSes and browsers to better protect users' private data
- Showed how to retrofit complex systems such as browsers to incorporate information flow control

Broader Impact:

- Tools we develop can help protect users' private data while interacting with these platforms
- Plan to develop browser extensions and web pages to raise public awareness of data privacy issues on these platforms
- Projects created training for 1 undergraduate researcher and 2 female graduate students