Toward Hybrid Enforcement of Security Policies in JavaScript Applications

Angel Luis Scull Pupo, Jens Nicolay
Elisa Gonzalez Boix

Context

- Static policy verification
- Dynamic policy enforcement
- Selective source code instrumentation

Objectives

- Hybrid program verification
- Reduce the runtime overhead introduced by monitoring the application

Implementation & Results

Input Program

$$G.onCall(document.write).deny();$$
$$document.write("foo"); //Disallow$$
$$document.createElement("div"); //Allow$$

Full Instrumentation

$$ADVICE.invoke(ADVICE.invoke(G, "onCall", [ADVICE.get(document, "write", 12)], 10), "deny", [\[]), 9);$$
$$ADVICE.invoke(document, "write", ["foo"], 15);$$
$$ADVICE.invoke(document, "createElement", ["div"], 19);$$

- Redundant instrumented code
- Redundant policy verifications
- Increased parse and load application time

Selective Instrumentation

$$G.onCall(document.write).deny();$$
$$ADVICE.invoke(document, "write", ["foo"], 10);$$
$$document.createElement("div");$$

- Less redundant policy checks
- Less instrumented code

Contact: Angel Luis Scull Pupo (ascullpu@vub.be), Jens Nicolay (jens.nicolay@vub.be) and Elisa Gonzalez Boix (egonzale@vub.be)